ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, september 2014

A Structure of Adaptive Portable Video Streaming and Efficient Common Video Cassette Sharing In the Clouds

M.Mahipal[1] M.Bhaskar[2]

[1]Student, Dept of Software Engineering, Vidyabharathi Institute of Technology, Warangal, Telangana, India

[2]HOD, Assistant Professor, Dept of Computer Science & Engineering, Vidyabharathi Institute of Technology, Warangal, Telangana, India

ABSTRACT: Utilizing the reasoning processing technology, a new cellular movie loading structure, known as AMES-Cloud, which has two main parts: AMoV (adaptive cellular movie streaming) and ESoV (efficient public movie sharing). AMoV and ESoV build a personal broker to offer movie loading services efficiently for each cellular customer. For a given customer, AMoV lets her undercover broker adaptively adjust her stream flow with a scalable movie programming technique in accordance with the reviews of link quality. Likewise, ESoV watches the online community communications among cellular users, and their personal providers try to prefetch movie content in advance. We apply a model of the AMES-Cloud structure to show its performance. It is shown that the personal providers in the atmosphere can effectively offer the flexible loading, and perform movie discussing (i.e., prefetching) in accordance with the online community analysis.. We first recommend an precise Comparison-based Profile Related method (eCPM) which runs between two parties, an initiator and a -responder. The eCPM enable the initiator to acquire the comparison-based matching outcome about a specified feature in their profiles, while stop their feature values from exposure. We then recommend an implied Comparison-based Profile Related method (iCPM) which allows the initiator to straight acquire some information instead of the evaluation outcome from the -responder. The information unique to customer profile can be separated into multiple groups by the -responder. The initiator unquestioningly selects the involved category which is unknown to the -responder.

KEYWORDS: AMES,AMOV,ESOV,ECPM,ICPM.

I. INTRODUCTION

While receiving movie loading traffic via 3G/4G cellular networks, cellular customers often suffer from long shield efforts and sporadic interruptions due to the limited data transfer useage and weblink situation fluctuation caused by multi-path adding and customer flexibility Thus, it is crucial to enhance the support high high quality of cellular movie loading while using the networking and estimate resources efficiently. Lately there have been many studies on how to enhance the support high high quality of cellular movie loading on two aspects:Scalability: Mobile movie loading military should assistance a wide variety of cellular devices; they have different movie solutions, different processing abilities, different wi-fi hyperlinks (like 3G and LTE) and so on. Also, the available weblink capacity of a cellular phone may vary eventually and area based on its signal strength, other customers traffic in the same cell, and weblink situation difference. Storing several versions (with different bit rates) of the same movie material may have high expense in terms of storage area and communication. To deal with this problem, the Scalable Video Programming (SVC) technique (Annex G extension) of the H.264 AVC movie pressure standard defines a first layer (BL) with several enhance layers (ELs). These sub sources can be secured by taking advantage of three scalability features: (i) spatial scalability by adding picture (screen pixels), (ii) temporary scalability by adding the frame amount, and (iii) high quality scalability by adding the picture pressure. By the SVC, video clips clip can be decoded/played at the lowest high quality if only the BL is provided. However, the more ELs can be provided, the better class of it clip flow is achieved.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, september 2014

Adaptability

Traditional movie loading methods designed by taking into consideration relatively constant traffic hyperlinks between servers and customers, perform badly in cellular surroundings [2]. Thus the fluctuating wi-fi weblink position should be properly dealt with to provide 'tolerable" movie loading solutions. To deal with this problem, we have to adjust it clip bit amount adjust to the currently time-varying available weblink data transfer useage of each cellular customer. Such flexible loading methods can successfully reduce bundle failures and data transfer useage waste. Scalable movie coding and flexible flow methods can be together combined to accomplish successfully the best possible high high quality of movie loading solutions. Thus the problem is that the server should take over the substantial processing expense, as the number of customers increases. have suggested to make customized brilliant providers for maintenance cellular customers, e.g., Cloudlet and Status. This is because, in the reasoning, many broker instances (or threads) can be maintained dynamically and efficiently based on the time-varying customer demands. Lately online community solutions (SNSs) have been popular. There have been suggestions to enhance the high high quality of material delivery using SNSs [23] [24]. In SNSs, customers may share, comment or re-post video clips among buddies and associates in the same team, which implies a customer may observe video clips clip that her buddies have recommended (e.g. [24]). Users in SNSs can also follow famous and accepted customers based on their interests (e.g., an official twitter or facebook account that shares the latest pop music videos), which is likely to be watched by its followers. In this regard, we are further inspired to manipulate the relationship among cellular customers from their SNS behavior to be able to prefetch in advance the beginning part of it clip or even the whole movie to the associates of a team who have not seen it clip yet. It can be done by a background job assistance by the broker (of a member) in the cloud; once the customer mouse clicks to discover the shocking truth, it can instantly begin to play. In this document, we design a flexible movie loading and prefetching structure for cellular customers with the above objectives in thoughts, known as AMES-Cloud. AMES-Cloud constructs a personal broker for each cellular customer in reasoning processing surroundings, which is used by its two main parts: (i) AMoV (adaptive cellular movie streaming), and ESoV (efficient public movie sharing). The efforts of this document can be described as follows:AMoV offers the best possible loading experiences by adaptively controlling the loading bit amount
depending on the fluctuation of the weblink high quality. AMoV adapts the bit amount for each customer utilizing the scalable movie coding. The personal broker of a customer keeps track of the reviews to be able on the weblink position. Private providers of customers are dynamically started and enhanced in the reasoning estimate platform. Also the real-time SVC coding is done on the reasoning processing side efficiently.

II. AMES-CLOUD FRAMEWORK

In this section we explain the AMES-Cloud framework includes the Adaptive Mobile Video stream (AMoV) and the Efficient Social Video sharing (ESoV). As shown in Fig. 1, the whole video storing and streaming system in the cloud is called the Video Cloud (VC). In the VC, there is a large-scale video base (VB), which stores the most of the popular video clips for the video service providers (VSPs). A sequential video base (tempVB) is used to cache new candidates for the popular videos, while tempVB counts the access frequency of each video. The VC keeps running a collector to seek videos which are by now popular in VSPs, and will re-encode the collected videos into SVC format and store into tempVB first. By this 2-tier storage, the AMES-Cloud can keep serving most of popular videos eternally. Note that management work will be handled by the manager in the VC. Specialized for each mobile user, a sub-video cloud (subVC) is created dynamically if there is any video streaming demand from the user. The sub-VC has a sub video base (subVB), which stores the recently fetched video segments. Note that the video deliveries among the subVCs and the VC in most cases are actually not "copy", but just "link" operations on the same file eternally within the cloud data center [36]. There is also encoding function in subVC (actually a smaller-scale encoder instance of the encoder in VC), and if the mobile user demands a new video, which is not in the subVB or the VB in VC, the subVC will fetch, encode and transfer the video. During video streaming, mobile users will always report link conditions to their corresponding subVCs, and then the subVCs offer adaptive video streams. Note that each mobile device also has a provisional caching storage, which is called local video base (localVB), and is used for buffering and prefetching.

A. Social Content Sharing

In SNSs, users subscribe to known friends, celebrities, and particular fascinated material marketers as well; also there are various types of community actions among customers in SNSs, such as immediate concept and community publishing. For growing video clips in SNSs, one can publish video clips clip in the community, and his/her members

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, september 2014

can easily see it; one can also straight suggest video clips clip to specified friend(s); furthermore one can regularly get observed by signed up material founder for new or well-known video clips. Just like research in [23] [24], we define different durability levels for those community actions to indicate the possibility that it clip distributed by one customer may be viewed by the devices of the one's discussing actions, which is known as a "hitting probability", so that subVCs can bring out effective qualifications prefetching at subVB and even localVB. Because after video clips clip discussing action, there may be a certain wait that the receiver gets to know the discussing, and triggers to look at [38]. Therefore the prefetching in prior will not effect the customers at most situations. Instead, a customer can just click to see without any streaming wait as the starting part or even the whole movie is already prefetched at the localVB. The amount of prefetched sections is mainly identified by the durability of the community actions. And the prefetching from VC to subVC only represents the "linking" action, so there is only file finding and connecting functions with small delays; the prefetching from subVC to localVB also relies on the durability of the community actions, but will also think the wi-fi weblink position.We categorize the community actions in present well-known SNSs into three types, regarding the effect of the actions and the prospective responding concern from the perspective of the recipient:

_ **Subscription**: Like the popular RSS services, an user can subscribe to a particular video publisher or a special video collection tune based on his/her interests. This interest-driven connectivity between the subscriber and the video publisher is considered as "median", because the subscriber may not always watch all subscribed videos.

_ **Direct recommendation**: In SNSs, an user directly recommend a video to particular friend(s) with a short message. The recipient of the message may watch it with very high probability. This is considered as "strong".

_ **Public sharing**: Each user in SNSs has a timeline-based of activity stream, which shows his/her recent activities. The activity of a user inspection or sharing a video can be seen by his/her friends (or followers). We consider this public distribution with the "weak" connectivity among users, because not many people may watch the video that one has seen without direct recommendation.

B. Prefetching Levels

Different strengths of the social activities point to different levels of probability that a video will be soon watched by the recipient. Correspondingly we also define three prefetching levels regarding the social activities of mobile users:

_ **"Parts":** Because the videos that published by subscriptions may be watched by the subscribers with a not high probability, we propose to only push a part of BL and ELs segment, for example, the first 10% segments.

_ "**All**": The video shared by the direct recommendations will be watched with a high probability, so we propose to prefetch the BL and all ELs, in order to let the recipient(s) directly watch the video with a good quality, without any buffering.

_ "**Little**": The public sharing has a weak connectivity among users, so the probability that a user's friends (followers) watch the video that the user has watch or shared is low. We propose to only prefetch the BL segment of the first time window in the opening to those who have seen his/her activity in the stream.The prefetching happens among subVBs and the VB, also more importantly, will be performed from the subVB to localVB of the mobile device depending on the link quality. If a mobile user is covered by Wi-Fi access, due to Wi-Fi's capable link and low price (or mostly for free), subVC can force as much as possible in most situations. However if it is with a 3G/4G relationship, which expenses a lot and experiences restricted data transfer useage, we recommend to restrict the prefetching stage to preserve power and price as detailed in Desk. 1, but customers can still benefit from the prefetching successfully. Observe that some power forecast technique can be implemented to be able to definitely choose whether present battery power position is appropriate for "parts" or "little" [39]. If a customer, A, gets the immediate suggestions of video clips clip from another customer, B, A's subVC will instantly prefetch it clip either from B's subVB, or from the VB at the stage of all if A is with Wi-Fi accessibility. However if customer A is linked with 3G/4G weblink, we will precisely prefetch a aspect of it clip department to A's regional storage space at the stage of "parts". Observe that the signed up video clips will be not prefetched when customer A is at 3G/4G relationship, as it is reduced from "little" tonone. A better expansion of the prefetching technique by public actions can be developed by an self-updating device from the user's reaching record in an transformative way. This learning-based prefetching is out of the opportunity of this document, and will be researched as our upcoming perform.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, september 2014

III. PROPOSED MODEL

EXPLICIT COMPARISON-BASED APPROACH

In this section, we present the explicit Comparison-based Profile Matching protocol, i.e., eCPM. This protocol allows two users to compare their attribute values on a specified attribute without disclose the values to each other. But, the protocol reveals the comparison result to the initiator, and therefore offers qualified anonymity.

a. Bootstrapping

The protocol has a fundamental bootstrapping phase, where the TCA generate all system parameters, user pseudonyms, and keying materials. Specifically, the TCA runs G to generate⟨p, q, R, R, χ⟩ for initiating the homomorphic encryption (see Sec. III-A). The TCA generates a pair of public and private keys ((pk_{TCA}, sk_{TCA}) for itself. The public key pk_{TCA} is open to all users; the private key sk_{TCA} is a secret which will be used to issue certificates for user pseudonyms and keying materials, as shown below. In this section, we propose the implicit Comparison-based Profile Matching (iCPM) by adopting the oblivious transfer cryptographic technique [40]. We consider users have distinct values for any given attribute. As shown in Fig. 3, the iCPM consists of three main steps. In the first step, u_i, chooses an involved category T_y by setting y-th element to 1 and other elements to 0 in a λ-length vector V_i. u_i, then encrypt the vector by using the homomorphic encryption and sends the encrypted vector to u_j. Thus, u_j is unable to know T but still can process on the cipher text. In the second step, u_j computes the ciphertexts with input of self-defined messages $(s_{1,h}, s_{0,h})$ for $1 \leq h \leq \lambda$, two encrypted vectors (m_i, d_i), and its own attribute value $a_{j,x}$. In the last step, u in the last step u_i, decrypts the cipher text and obtain $s_{1,y}$ if $a_{i,x} > a_{j,x}$ or $s_{0,y}$ if $a_{i,x} < a_{j,x}$.

a.Protocol Steps

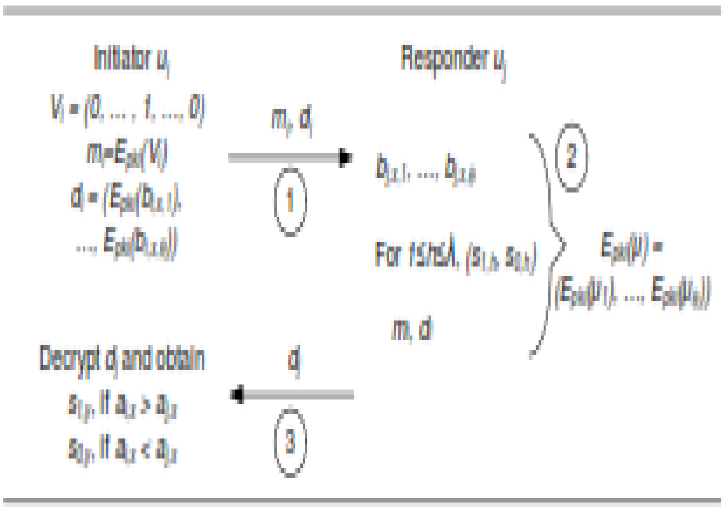


Fig. : The iCPM flow

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, september 2014

Step 1. u_i generates a vector $V_i = (v_1, \cdots, v_\lambda)$, where $v_y = 1$ and $v_h = 0$ for $1 \le h \le \lambda$ and $h \ne y$. This vector implies that u_i is interested in the category T_y. u_i sets $m_i = E_{pk_i}(V_i) = (E_{pk_i}(v_1), \cdots, E_{pk_i}(v_\lambda))$. It converts $a_{i,x}$ to binary bits $\langle b_{i,x,1}, \cdots, b_{i,x,\theta}\rangle$, where $\theta = \lceil \log l \rceil$, and sets $d_i = (E_{pk_i}(b_{i,x,1}), \cdots, E_{pk_i}(b_{i,x,\theta}))$. It sends a 6-tuple $(pid_i, cert_{pid_i}, a_x, d_i, m_i, Sign_{psk_i}(a_x, d_i, m_i))$ to u_j.

Step 2. After receiving the 6-tuple, u_j checks if $(pid_i, cert_{pid_i})$ are generated by the TCA and the signature is generated by u_i. If both checks are successful, it knows that (a_x, d_i, m_i) is valid. u_j proceeds as follows:

1) Convert $a_{j,x}$ to binary bits $\langle b_{j,x,1}, \cdots, b_{j,x,\theta}\rangle$ and compute $E_{pk_i}(b_{j,x,t})$ for $1 \le t \le \theta$.
2) Compute $e'_t = E_{pk_i}(b_{i,x,t}) - E_{pk_i}(b_{j,x,t}) = E_{pk_i}(\zeta'_t)$.
3) Compute $e''_t = (E_{pk_i}(b_{i,x,t}) - E_{pk_i}(b_{j,x,t}))^2 = E_{pk_i}(\zeta''_t)$.
4) Set $\gamma_0 = 0$, and compute $E_{pk_i}(\gamma_t)$ as $2E_{pk_i}(\gamma_{t-1}) + e''_t$, which implies $\gamma_t = 2\gamma_{t-1} + \zeta''_t$.
5) Select a random $r_t \in R_p$ in the form of $ax + b$ where $a, b \in \mathbb{Z}_p, a \ne 0$, and compute $E_{pk_i}(\delta_t)$ as $E_{pk_i}(\zeta'_t) + E_{pk_i}(r_t) \times (E_{pk_i}(\gamma_t) - E_{pk_i}(1))$, which implies $\delta_t = \zeta'_t + r_t(\gamma_t - 1)$.
6) Select a random $r_p \in \mathbb{Z}_p$ $(r_p \ne 0)$, and compute $E_{pk_i}(\mu_t)$ as

$$\sum_{h=1}^{\lambda}((s_{1,h} + s_{0,h})E_{pk_i}(1) + s_{1,h}E_{pk_i}(\delta_t) - s_{0,h}E_{pk_i}(\delta_t))$$
$$\times (r_p((E_{pk_i}(v_h))^2 - E_{pk_i}(v_h)) + E_{pk_i}(v_h))$$
$$+ r_p(\sum_{h=1}^{\lambda} E_{pk_i}(v_h) - E_{pk_i}(1)),$$

which implies $\mu_t = \sum_{h=1}^{\lambda}(s_{1,h}(1+\delta_t) + s_{0,h}(1-\delta_t))((v_h^2 - v_h)r_p + v_h) + (\sum_{h=1}^{\lambda} v_h - 1)r_p$.

Then, u_j compiles $E_{pk_i}(\mu) = (E_{pk_i}(\mu_1), \cdots, E_{pk_i}(\mu_\theta))$, and makes a random permutation to obtain $d_j = \mathcal{P}(E_{pk_i}(\mu))$. It finally sends a 5-tuple $(pid_j, cert_{pid_j}, a_x, d_j, Sign_{psk_j}(a_x, d_j))$ to u_i.

Step 3. u_i checks the validity of the received 5-tuple. Then, it decrypts every ciphertext $E_{pk_i}(\mu_t)$ in d_j as follows: for $E_{pk_i}(\mu_t) = (c_0, \cdots, c_\alpha)$, obtain μ_t by $\mu_t = (\sum_{h=0}^{\alpha} c_h s^h)$ mod p. If $a_{i,x} > a_{j,x}$, u_i is able to find a plaintext $\mu_t \in \mathbb{Z}_p$ and $\mu_t = 2s_{1,y} \le p-1$ and computes $s_{1,y}$; if $a_{i,x} < a_{j,x}$, u_i is able to find $\mu_t = 2s_{0,y}$ and computes $s_{0,y}$.

b.Effectiveness Discussion

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, september 2014

The correctness of the iCPM can be verified as follows. If $a_{i,x} > a_{j,x}$, then there must exist a position, say the t^*-th position, in the binary expressions of $a_{i,x}$ and $a_{j,x}$ such that $b_{i,x,t^*} = 1, b_{j,x,t^*} = 0$ and $b_{i,x,t'} = b_{j,x,t'}$ for all $t' < t^*$. Since $\gamma_t = 2\gamma_{t-1} + \zeta''_t$, we have $\gamma_{t'} = 0$, $\gamma_{t^*} = 1$, and $\delta_{t^*} = 1$. For $t'' > t^*$, we have $\gamma_{t''} \geq 2$, and δ_t is a random value due to $r_{t''}$. Since $s_{0,y}$ and $s_{1,y}$ are elements of $\mathbb{Z}_p$ and r_t is in the form of $ax + b$ $(a, b \in \mathbb{Z}_p, a \neq 0)$, u_i can always determine the effective plaintext from others. The effective plaintext will be $\mu_t = \sum_{h=1}^{\lambda}(s_{1,h}(1 + \delta_{t^*}) + s_{0,h}(1 - \delta_{t^*}))((v_h^2 - v_h)r_p + v_h) + (\sum_{h=1}^{\lambda} v_h - 1)r_p$. If the vector V_i from u_i does not satisfy $\sum_{h=1}^{\lambda} v_h = 1$ or $v_h \in \{0, 1\}$, u_i cannot remove the random factor r_p; if V_i satisfies the conditions, only $s_{1,y}$ and $s_{0,y}$ will be involved in the computation. Because $\delta_{t^*} = 1$, u_i can obtain $\mu_t = 2s_{1,y} \leq p-1$ and recovers $s_{1,y}$. If $a_{i,x} < a_{j,x}$, we similarly have $\mu_t = 2s_{0,y}$ and u_i can obtain $s_{0,y}$.

The confidentiality of customer profiles is certain by the homomorphic security. The evaluation outcome is always in the secured structure, and is not straight revealed to The exposed details is either or which is irrelevant to customer profiles. Therefore, the method get in touch with do not help in wondering the profiles, and the complete privacy is offered. Meanwhile, vector is always in an secured structure so that is incapable to know the fascinated type of . Moreover, guarantees that only one of and will be exposed to The non-forgeability residence is just like that of the eCPM. will not lie as it creates trademark) and gives it to . The profile bogus strike will be recognized if reviews the trademark to the TCA. Moreover, has no need to lie as it can accomplish the same purpose by basically change the material of and.

IV. IMPLICIT PREDICATE-BASED APPROACH

Both the eCPM and the iCPM perform profile matching on a single attribute. For a matching connecting multiple attributes, they have to be executed multiple times, each time on one attribute. In this section, we extend the iCPM to the multi attribute cases, without jeopardizing its anonymity property, and obtain an implicit Predicate-based Profile Matching protocol, i.e., iPPM. This protocol relies on a predicate which is a logical expression made of multiple comparisons across distinct attributes and thus supports complicated matching criteria within a single protocol run. As shown in Fig. the iPPM is composed of three main steps. In the first step, dissimilar from the iCPM, u_i, n encrypted vectors of its attribute values corresponding to the attributes in A where A (|A| = n = w) is the attribute set of the predicate _. In the second step, u_j sets 2λ polynomial functions $f_{sat,h}(x), f_{unsat,h}(x)$ for $1 \leq h \leq \lambda$. u_j generates 2λn secret shares from $f_{sat,h}(x), f_{unsat,h}(x)$ by chossing $1 \leq h \leq \lambda, 1 \leq x \leq n$, and arranges them in a certain structure according to the predicate For every 2λ secret shares with the same index h, similar to the step 2 of the iCPM, u_j generates θ ciphertexts. u_j sends to u_i, obtains nθ ciphertexts at the end of the second step. In the third step, u_j decrypts these nθ ciphertexts and finds n secret shares of finally can obtain $s_{1,y}$ or $s_{0,y}$ from the secret shares.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, september 2014

a.Protocol Steps

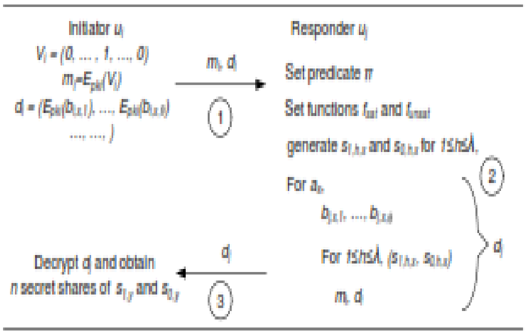


Fig.: The iPPM flow

The iPPM is obtained by combining the iCPM with a secret sharing scheme to support a predicate matching. The initiator u_i sends its attribute values matching to the attributes in A to the responder u_i. Without loss of generality, we assume $A = \{a_1, \cdots, a_n\}$. Then, u_j defines a predicate $\Pi =$ "$\bar{t}$ of $\{(a_{i,x}, opt, a_{j,x}) | a_x \in A\}$". where the comparison operator opt is either > or < and $1\bar{t} \le n$. The predicate contains n number of requirements (i.e., comparisons), each for a distinct a The responder u_i determine λ pairs of messages $(s_{0,h}, s_{1,h})$ receives $s_{1,h}$ for attributes a_h $(1 \le h \le \lambda)$. The initiator u_i if at least $\bar{t}$ of the n requirements are satisfied, otherwise. Similar to the iCPM, T_y but unknown to u_j is determined by u_i. The threshold gate $1 \le \bar{t} \le n$ is chosen by When n = 1, the iPPM reduces to the iCPM. The protocol steps are given below.

Step 1. u_i generates a vector $V_i = (v_1, \cdots, v_\lambda)$, where $v_y = 1$ and $v_h = 0$ for $1 \le h \le \lambda$ and $z \ne y$, and sets $m_i = E_{pk_i}(V_i) = (E_{pk_i}(v_1), \cdots, E_{pk_i}(v_\lambda))$. In addition, u_i selects the attribute set A ($|A| = n$), and sends a 6-tuple $(pid_i, cert_{pid_i}, A, d_i, m_i, Sign_{psk_i}(A, d_i, m_i))$ to u_j, where d_i contains $n\theta$ ($\theta = \lceil \log l \rceil$) ciphertexts as the homomorphic encryption results of each bit of $a_{i,x}$ for $a_x \in A$.

Step 2. u_j checks the validity of the received 6-tuple (similar to the Step 2 of the iCPM). It creates a predicate Π and chooses the threshold gate $\bar{t}$. Using the secret sharing scheme [46], u_j creates 2λ polynomials: $f_{sat,h}(v) = \rho_{\bar{t}-1,h} v^{\bar{t}-1} + \cdots + \rho_{1,h} v + s_{1,h}$ and $f_{unsat,h}(v) = \rho'_{n-\bar{t},h} v^{n-\bar{t}} + \cdots + \rho'_{1,h} v + s_{0,h}$ for $1 \le h \le \lambda$, where $\rho_{\bar{t}-1,h}, \cdots, \rho_{1,h}, \rho'_{n-\bar{t},h}, \cdots, \rho'_{1,h}$ are random numbers from $\mathbb{Z}_p^*$. For each attribute $a_x \in A$, it calculates the secret shares of $s_{1,h,x}$ and $s_{0,h,x}$ as follows

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, september 2014

$(s_{1,h,x}, s_{0,h,x} \leq (p-1)/2$ are required):

$$\begin{cases} s_{0,h,x} = 0||f_{unsat,h}(x), & \\ s_{1,h,x} = 1||f_{sat,h}(x), & \text{if "}a_{i,x} > a_{j,x}\text{"} \in \Pi; \\ s_{0,h,x} = 1||f_{sat,h}(x), & \\ s_{1,h,x} = 0||f_{unsat,h}(x), & \text{if "}a_{i,x} < a_{j,x}\text{"} \in \Pi. \end{cases}$$

Note that u_j adds a prefix 0 or 1 to each secret share such that u_i is able to differentiate the two sets of shared secrets, one for $s_{1,h}$, the other for $s_{0,h}$. u_j runs the Step 2 of the iCPM n times, each time for a distinct attribute $a_x \in \mathcal{A}$ and with $(s_{1,h,x}, s_{0,h,x})$ for $(1 \leq h \leq \lambda)$ being input as $s_{1,h}$ and $s_{0,h}$, respectively. u_j then obtains d_j including $n\theta$ ciphertexts. Finally, it sends a 6-tuple $(pid_j, cert_{pid_j}, \bar{t}, \mathcal{A}, d_j, Sign_{psk_j}(d_j))$ to u_i.

Step 3. u_i checks the validity of the received 6-tuple. u_i can obtain n secret shares, and each of these shares is either for $s_{0,y}$ or $s_{1,y}$. It then classifies the n shares into two groups by looking at the starting bit (either '0' or '1'). Thus, if Π is satisfied, u_i can obtain at least $\bar{t}$ secret shares of $s_{1,y}$ and be able to recover $s_{1,y}$; otherwise, it must obtain at least $n-\bar{t}+1$ secret shares of $s_{0,y}$ and can recover $s_{0,y}$.

b. Effectiveness Discussion

The correctness of the iPPM is as follows. At Step 2, the responder u_i executes the Step 2 of the iCPM n times, each time it effectively delivers only one secret share of either $s_{0,y}$ or $s_{1,y}$ or u_i When u_i receives either $\bar{t}$ shares of $s_{1,y}$ or $n-\bar{t}+1$ shares of $s_{0,y}$, it can recover either $s_{1,y}$ or $s_{0,y}$. The interpolation function corresponding to the secret sharing scheme always guarantees the correctness. The anonymity and non-forgeability of the iPPM are achieved similar to those of the iCPM and the eCPM, respectively.

V. PERFORMANCE EVALUATION

The eCPM+ details accumulative privacy threat in several method operates and music itself instantly to maintain preferred privacy durability. Some past works are involved only with the privacy threat introduced by each individual method run, and some performs reduce privacy threat by personally modifying certain limit principles. Though they provide the depending privacy as the eCPM, they are not much like the eCPM and the eCPM+ because the privacy protection of customers is considered with regards to successive method operates. Therefore, in this area we assess the eCPM+ (which uses a pre-adaptive pseudonym modify strategy) in evaluation with two other eCPM versions, respectively utilizing a continuous pseudonym modify period (CONST-z) and a post-adaptive pseudonym modify technique (Post).

Simulation Setup

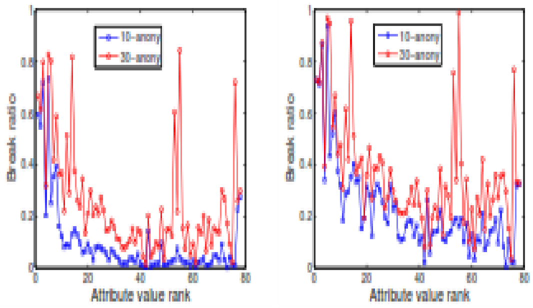
Our simulator research is in accordance with the real track [48] gathered from 78 customers participating a meeting during a four-day interval. A get in touch with indicates that two customers come near to each other and their connected Wireless gadgets identify each other. The users' Wireless gadgets run a finding system every 120 a few moments on regular and signed about 128, 979 connections. Each get in touch with is recognized by two customers, a start-time, and a length. In CONST-z, we set the pseudonym modify interval z from 1 to 40 (time slots); in the post-adaptive and pre-adaptive techniques, we set pseudonym life-time aspect $\xi = 30$. In the pre-adaptive

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

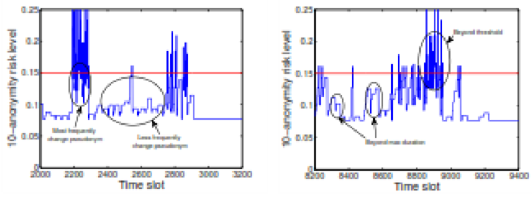
Vol. 2, Issue 9, september 2014



(a) $z = 1$ (b) $z = 20$

strategy, we use ARMA order (10, 5).

Anonymity break period under the constant strategy anonymity break period experienced by each user with the constant strategy being used. It can be seen that when z = 1, each user experiences the shortest anonymity break period at the cost of 10, 000 pseudonyms per user. Anonymity break is still possible in this extreme case because users may have multiple contacts within a single time slot while they are still using the same pseudonym. If a user has a more restrictive anonymity requirement (e.g., from 10-anonymity to 30-anonymity) or uses a larger pseudonym change interval (from 1 time slot to 20 time-slots), it will have more corrupted pseudonyms and thus suffer a longer period of anonymity break.



(a) Time period (2000, 3200) (b) Time period (8200, 9400)

Anonymity risk level over time (th = 0.15)

We choose the 32nd customer, who in common has lower privacy threat stage than the 7th customer, and show its 10-anonymity threat stage in two successive time times (2000, 3200) and (8200, 9400) with the post-adaptive technique in Fig. The privacy threat stage limit is th = 0.15. In the figure, the fall from a risky stage to a low threat stage indicates Remember that a customer changes its pseudonym not only when the privacy threat stage is beyond limit th but also when its current pseudonym ends. This is reflected by the privacy threat stage fall occurred below the limit line in the figure. From Fig we can see that the pseudonym change regularity is great when the customer activities a huge variety of others who live nearby. This is affordable as a huge variety of profile related operates are implemented in this case, and the user's privacy threat stage develops quickly. When the stage is beyond a pre-defined limit, the customer changes its pseudonym.

VI. CONCLUSION

We have examined a exclusive comparison-based profile related issue in Cellular Public Systems (MSNs), and suggested novel methods to fix it. The precise Comparison based Profile Matching (eCPM) method provides depending privacy. It shows the evaluation outcome to the initiator. Consider the k-anonymity as a customer need, we evaluate the privacy threat stage in regards to the pseudonym change for successive eCPM operates. We have further presented an improved edition of the eCPM, i.e., eCPM+, by taking advantage of the prediction-based technique and implementing the pre-adaptive pseudonym modify. The potency of the eCPM+ is verified through comprehensive models using real-trace details. We have also developed two methods with complete privacy, i.e., implied Comparison-based Profile Matching (iCPM) and implied Predicate-based Profile Matching (iPPM). The iCPM manages profile related depending on only one evaluation of an feature while the iPPM is applied with a sensible appearance made of several evaluations

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, september 2014

comprising several features. The iCPM and the iPPM both allow customers to anonymously demand for details and react to the demands according to the profile related outcome, without exposing any profile details.

VII. REFERENCES

[1]"Comscore,"http://www.comscoredatamine.com/.
[2] A. G. Miklas, K. K. Gollu, K. K. W. Chan, S. Saroiu, P. K. Gummadi, and E. de Lara, "Exploiting social interactions in mobile systems," in Ubicomp, 2007, pp. 409–428.
[3] S. Ioannidis, A. Chaintreau, and L. Massoulie, "Optimal and scalable distribution of content updates over a mobile social network," in Proc. IEEE INFOCOM, 2009, pp. 1422–1430.
[4]R. Lu, X. Lin, and X. Shen, "Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in Proc. IEEE INFOCOM, 2010, pp. 632–640.
[5] W. He, Y. Huang, K. Nahrstedt, and B. Wu, "Message propagation in adhoc-based proximity mobile social networks," in PERCOM workshops, 2010, pp. 141–146.
[6] D. Niyato, P. Wang, W. Saad, and A. Hjørungnes, "Controlled coalitional games for cooperative mobile social networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 4, pp. 1812–1824, 2011.
[7]M. Motani, V. Srinivasan, and P. Nuggehalli, "Peoplenet: engineering a wireless virtual social network," in MobiCom, 2005, pp. 243–257.
[8] M. Brereton, P. Roe, M. Foth, J. M. Bunker, and L. Buys, "Designing participation in agile ridesharing with mobile social software," in OZCHI, 2009, pp. 257–260.
[9] E.Bulut and B.Szymanski, "Exploiting friendship relations for efficient routing in delay tolerant mobile social networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 12, pp. 2254–2265, 2012.
[10] Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, and D. Li, "E-smalltalker: A distributed mobile system for social networking in physical proximity," in ICDCS, 2010, pp. 468–477.
[11] Q. Li, S. Zhu, and G. Cao, "Routing in socially selfish delay tolerant networks," in Proc. IEEE INFOCOM, 2010, pp. 857–865.
[12] X. Liang, X. Li, T. H. Luan, R. Lu, X. Lin, and X. Shen, "Moralitydriven data forwarding with privacy preservation in mobile social networks," IEEE Transactions on Vehicular Technology, vol. 7, no. 61, pp. 3209–3222, 2012.
[13] R. Gross, A. Acquisti, and H. J. H. III, "Information revelation and privacy in online social networks," in WPES, 2005, pp. 71–80.
[14] F. Stutzman, "An evaluation of identity-sharing behavior in social network communities." iDMAa Journal, vol. 3, no. 1, pp. 10–18, 2006.
[15] K. P. N. Puttaswamy, A. Sala, and B. Y. Zhao, "Starclique: guaranteeing user privacy in social networks against intersection attacks," in CoNEXT, 2009, pp. 157–168.
[16] E. Zheleva and L. Getoor, "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles," in WWW, 2009, pp. 531–540.
[17] G. Chen and F. Rahman, "Analyzing privacy designs of mobile social networking applications," IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, vol. 2, pp. 83–88, 2008.
[18] D. Balfanz, G. Durfee, N. Shankar, D. K. Smetters, J. Staddon, and H.C. Wong, "Secret handshakes from pairing-based key agreements," in IEEE Symposium on Security and Privacy, 2003, pp. 180–196.
[19] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in EUROCRYPT, 2004, pp. 1–19.
[20] R. Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake scheme with symptoms-matching for mhealthcare social network," ACM Mobile Networks and Applications (MONET), vol. 16, no. 6, pp. 683–694, 2011.
[21] M. Li, N. Cao, S. Yu, and W. Lou, "Findu: Privacy-preserving personal profile matching in mobile social networks," in Proc. IEEE INFOCOM, 2011, pp. 2435–2443.
[22] R. Zhang, Y. Zhang, J. Sun, and G. Yan, "Fine-grained private matching for proximity-based mobile social networking," in Proc. IEEE INFOCOM, 2012, pp. 1969–1977.
[23] W. Dong, V. Dave, L. Qiu, and Y. Zhang, "Secure friend discovery in mobile social networks," in Proc. IEEE INFOCOM, 2011, pp. 1647–1655.
[24] J. Freudiger, M. H. Manshaei, J.-P. Hubaux, and D. C. Parkes, "On noncooperative location privacy: a game-theoretic analysis," in ACM CCS, 2009, pp. 324–337.
[25] R. Lu, X. Lin, H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," IEEE Transactions on Vehicular Technology, vol. 61, no. 1, pp. 86 – 96, 2011.
[26] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in EUROCRYPT, 2008, pp. 146–162.
[27] N. Eagle and A. Pentland, "Social serendipity: mobilizing social software," IEEE Pervasive Computing, vol. 4, no. 2, pp. 28–34, 2005.
[28] J. Teng, B. Zhang, X. Li, X. Bai, and D. Xuan, "E-shadow: Lubricating social interaction using mobile phones," in ICDCS, 2011, pp. 909–918.
[29] B. Han and A. Srinivasan, "Your friends have more friends than you do: identifying influential mobile users through random walks," in MobiHoc, 2012, pp. 5–14.
[30] Z. Yang, B. Zhang, J. Dai, A. C. Champion, D. Xuan, and D. Li, "E-smalltalker: A distributed mobile system for social networking in physical proximity," in ICDCS, 2010, pp. 468–477.
[31] L. Kissner and D. X. Song, "Privacy-preserving set operations," in CRYPTO, 2005, pp. 241–257.
[32] Q. Ye, H. Wang, and J. Pieprzyk, "Distributed private matching and set operations," in ISPEC, 2008, pp. 347–360.
[33] D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, "Efficient robust private set intersection," in ACNS, 2009, pp. 125–142.
[34] S. Jarecki and X. Liu, "Efficient oblivious pseudorandom function with applications to adaptive ot and secure computation of set intersection," in TCC, 2009, pp. 577–594.
[35] C. Hazay and Y. Lindell, "Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries," Journal of Cryptology, vol. 23, no. 3, pp. 422–456, 2010.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 9, september 2014

[36] B. Goethals, S. Laur, H. Lipmaa, and T. Mielik ainen, "On private scalar product computation for privacy-preserving data mining," in ICISC, 2004, pp. 104–120. 2004, pp. 104–120.
[37] A. C.-C. Yao, "Protocols for secure computations (extended abstract)," in FOCS, 1982, pp. 160–164.
[38] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority," in STOC, 1987, pp. 218–229.
[39]
I. Ioannidis, A. Grama, and M. J. Atallah, "A secure protocol for computing dot-products in clustered and distributed environments," in ICPP, 2002, pp. 379–384.
[40] I. F. Blake and V. Kolesnikov, "Strong conditional oblivious transfer and computing on intervals," in ASIACRYPT, 2004, pp. 515–529.
[41] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in EUROCRYPT, 1999, pp. 223–238.
[42] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" in CCSW, 2011, pp. 113–124.
[43] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1621–1631, 2012.
[44] H. Ltkepohl, New introduction to multiple time series analysis. Springer, 2005.
[45] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, "Exploiting prediction to enable secure and reliable routing in wireless body area networks," in Proc. IEEE INFOCOM, 2012, pp. 388–396.
[46] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, 1979.
[47] L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 557–570, 2002.
[48] J. Scott, R. Gass, J. Crowcroft, P. Hui, C. Diot, and A. Chaintreau, "CRAWDAD trace cambridge/haggle/imote/infocom (v. 2006-01-31)," Jan. 2006.
[49] D. J. Watts, "Small worlds: The dynamics of networks between order and randomness," J. Artificial Societies and Social Simulation, vol. 6, no. 2, 2003.
[50] C. Bron and J. Kerbosch, "Finding all cliques of an undirected graph (algorithm 457)," Communications of the ACM, vol. 16, no. 9, pp. 575–576, 1973.