M-SRS: Secure and Trustworthy Mobile Service Review System Based on Mobile Cloudlet

Tao Jiang, Xiaofeng Chen, Jin Li, Jianfeng Ma

M-SRS: Secure and Trustworthy Mobile Service Review System Based on Mobile Cloudlet

Tao Jiang[1], Xiaofeng Chen[1⋆], Jin Li[2], and Jianfeng Ma[1]

[1] State Key Laboratory of Integrated Service Networks (ISN), Xidian University, Xi'an, P.R. China
jiangt2009@gmail.com, {xfchen, jfma}@xidian.edu.cn
[2] School of Computer Science, Guangzhou University, China
lijin@gzhu.edu.cn

Abstract. The scope of services has skyrocketed to such an extent that it is necessary for the service consumers to quickly understand the quality of a service provided by different vendors through Service Review Systems (SRS). In this paper, we consider the trustworthyness of a SRS without a trusted review management center in location-based Service-oriented Mobile Social Networks (S-MSNs). Firstly, we broach some review statistic modification attacks, which are very important for service consumers to review a service. Secondly, the M-SRS network model based on Mobile Cloud Computing (MCC) is constructed, which could protect the security and reduce the communication and computation overhead. Also, data entanglement and verifiable service utilization tickets are adopted to prevent proposed attacks in existing SRS and guarantee the trustworthyness of the statistic SRS. Final results show that M-SRS could effectively resist the existing service review attacks, and it is efficient in terms of review submission and review authenticity verification for the whole system.

Keywords: cloud computing; mobile social networks; location-based service; service review; security; trustworthyness.

1 Introduction

Service review system (SRS) is designed to identify potential service delivery improvements, which contains the feedback of users such as compliments and complains about the services or products from service consumers. Typically, SRS is maintained by a trusted part in some popular Internet based social network such as Facebook. Unlike those global wide service whose service reviews are maintained by a trusted third part, the local service providers are interested mainly in their geographic vicinity and maintain a SRS by themselves.

Service-oriented Mobile Social Networks (S-MSNs) are composed of static service providers (vendors) and mobile service consumers (users). The vendors,

⋆ Corresponding author

such as restaurants and grocery stores, can provide Location-Based Services (LBSs) for mobile users. The LBSs can be embedded into various kinds of networks to obtain different applications [7, 8, 13, 14]. The security and privacy problems of LBSs in MSN have been widely discussed [1,3,11,15]. On the contrary, in this paper, we mainly consider the security and privacy of SRSs managed by a selfish vendor, in which the vendor may be incented to conduct malicious activity on the reviews. Aiming at this problem, Liang et al. [10] designed a scheme SEER to protect against a selfish vendor from rejecting or deleting negative reviews or inserting forged positive ones to increase its reputation.

Based on SEER, we further study the fundamental security challenges of the SRSs without trust review managers.Correlation analysis of SEER shows that it is impossible for the vendor to drop or modify a review according to the ring structure, and the scheme has high submission rate and low submission delay. However, we find that, in SEER, a malicious vendor could always do the selective review deletion of rings that provide the negative effect, and there is no mechanism to check whether the reviews of some rings submitted before are deleted by the vendor. Also, the SRS that provides general ratings is not secure against the review statistical results forgery attack.

In this paper, we present general framework for secure and efficient SRS based on data entanglement. In our framework, mobile cloudlet, identity based aggregate signature could be adopted to improve the efficiency of our schemes, and the pseudonym technology is a secretive module for protecting the privacy of users in the SRS. It is shown that our entangled review submission method provides a strong protection on all reviews. The malicious activity of a vendor will be found with a very high probability, even if a small fraction of the reviews is destroyed. Specially, when each user provides an entanglement of 10 reviews, about 40 users, who submit reviews, will detect the malicious behavior of the vendor with 99% probability, when only 1% reviews are destroyed. The probability that a vendor conducts malicious activity on users' reviews, without being detected, decreases with the increase of new reviews submission.

2 Preliminaries

Let k be the security parameter and H be a cryptographic hash function. In addition, we make use of a pseudo-random permutation (PRP) π with the following parameters: $\pi : \{0,1\}^k \times \{0,1\}^{log_2(n)} \rightarrow \{0,1\}^{log_2(n)}$. We write $\pi_k(x)$ to denote π keyed with key k applied on input x.

Bilinear Maps: Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of some large prime order q. We write $\mathbb{G}_1$ additively and $\mathbb{G}_2$ multiplicatively. We will call $\hat{e}$ an admissible pairing if $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a map with the following properties:

1. Bilinear: $\hat{e}(aQ, bR) = \hat{e}(Q, R)^{ab}$ for all $Q, R \in \mathbb{G}_1$ and all $a, b \in \mathbb{Z}$.
2. Non-degenerate: $\hat{e}(Q, R) \neq 1$ for some $Q, R \in \mathbb{G}_1$.
3. Computable: There is an efficient algorithm to compute $\hat{e}(Q, R)$ for any $Q, R \in \mathbb{G}_1$.

Since $\hat{e}$ is bilinear and $\mathbb{G}_1$ is a cyclic group, it means that $\hat{e}$ is also symmetric. Then, we get $\hat{e}(Q, R) = \hat{e}(R, Q)$ for all $Q, R \in \mathbb{G}_1$.

3 Network Model and Attacks

In this section, the network model of S-MSN is described, over which we further propose our M-SRS.

3.1 Network Model

S-MSN is a network consists of multiple vendors that provide services to users, in which vendors maintain an SRS independently for themselves to provide public servers reviews for the services they provide. The vendor is equipped with a static wireless communication device and it has a large storage space and computational capabilities. Each user has a hand-held device with smaller communicational transmission range and computational capabilities than that of the vendor.

Users spontaneously form different social groups according to their common interests in an S-MSN. We suppose that there are v social groups $\{G_1, ..., G_v\}$ and denote I_u the universal interest set. Also, we denote the interest set of a social group G_i by $I_i (I_i \subseteq I_u)$ for $1 \leq i \leq u$. Each user u_j belongs to at least one social group and it inherits the interests of those social groups. Thus, the interest set of u_j is $S_j = \cup_i I_i$, where u_j is a member of G_i. The vendors, tagged by interests, periodically disseminate their up-to-date service information including service description and reviews to users. The integrity and unforgeability of such service information will be ensured by using a public/private key pairs of the vendors.

The membership management of every group $G_i (1 \leq i \leq u)$ is relied on an offline trusted authority TA. It has a public/private key pair (pk, sk), and publishes the public key to all users. Every user u_j has a unique identity ID_j and it is used for the TA to verify the validity of u_j when u_j joins group G_i.

In our network model, there are four entities, namely the users, the vendors, the mobile cloudlet (MC) composed of users and a trusted authority (TA).

3.2 Attack Model

The vendor will be able to conduct the following statistical review attacks:

- **Colluded Review Injection Attack:** Colluded review injection attack is launched by the vendor, where the selfish vendor conspires with some malicious users and submits some positive reviews without being detected.
- **Selective Review Delete Attack:** Selective review delete attack is conducted by a malicious vendor by deleting one or a set of target reviews in the service review system, where a vendor could find out and delete those negative reviews without being detected.

– **Review Statistical Results Forgery Attack:** Review statistical results forgery is an attack conducted by malicious vendors. In the attack, a malicious vendor will just provide a false statistical result of its service when the number of reviews in the SRS is too large and the users are not able or unwilling to calculate.

4 The M-SRS System

In this section, we elaborate on review entanglement based on mobile cloudlet and then describe the detail processes of the review generation and submission in M-SRS.

4.1 Reviews Entanglement and Mobile Cloudlet

In our M-SRS, to prevent from a lucrative opportunity in altering or simply neglecting to keep the negative review result in M-SRS, we adopt review entanglement to link the fate of reviews. Thus, according to the definition of *entangled* in [2], the fate of a review will be linked to at least t other reviews that a malicious vendor cannot hope to offend them all with impunity.

We adopt mobile cloudlets [12] to serve users, which is one network structure of the mobile cloud computing (MCC) [4, 5, 9]. It is a small cloud composed through the cooperation of mobile users and vendors nearby. The mobile cloudlet will assist the users to transmit or verify the message of users and vendors in our network. We assume that the public users are justice and it is difficult for a vendor to bribe all the users in the cloudlet. Thus, we consider that the cloudlet will always provide trusted activity in the processes of reviews submission of users in our M-SRS.

4.2 Constructions

The details of the construction of our M-SRS are elaborated as follows.

System Setup. The system setup phase initializes the necessary parameters in the following two steps:

Step1: The member management of a group relies on the offline trusted authority TA. TA initializes its public/private key pair (pk_{TA}, sk_{TA}) and publishes the public key pk_{TA} to all users in the network.

Step2: Every user u_j has a unique identity ID_j when an identity based signature scheme [6] is adopted to implement the membership of the system. When u_j joins the G_h, TA will verify the validity of the identity ID_j of u_j. We will identify the user as $ID_{h,j}$, when user ID_j joins a group G_h.

Review Generation and submission. After being served by a vendor V, a user u_j will get a ticket TK as an evidence to prove that the user does enjoy the service and has the right to submit its review for the service. When u_j wants to generate a review for the service, it conducts a review generation process in the following steps.

Step1: The user u_j generates a random seed s. On inputting s, u_j computes coefficients $a_i = \pi_s(i)$ where $1 \leq i \leq t$.

Step2: When the vendor is within the communication range,

1. u_j will directly send the seed s to the vendor V in a verifiable message $Msg_{h,j} = ID_{h,j}|ID_V|\ TK_{h,j}|s_{h,j}|T_{h,j}|\sigma_{h,j}$ where $T_{h,j}$ is current time stamp and $\sigma_{h,j} = Sign_{sk_{h,j}}(ID_{h,j}|\ ID_V|TK_{h,j}|s_{h,j}|T_{h,j,1})$ is the signature of the content of the message using its secret key $sk_{h,j}$. Otherwise, the seed s will be sent to the vendor through the mobile cloudlet around the vendor in an indirect way as shown in Step 3.
2. When V receives $Msg_{h,j}$, it will check the validity of the$Msg_{h,j}$ and $TK_{h,j}$. If both of the $Msg_{h,j,1}$ and $TK_{h,j}$ pass the validity test, V will compute coefficients $a_i = f_s(i)$ where $1 \leq i \leq t$ and send the review set $REV_{a_i}(1 \leq i \leq t)$, and the last review REV_N in the system to the u_j as shown bellow.

$$REV_{a_i} = KID|ID_{u,j}|ID_V|TK_{a_i}|s_{a_i}|T_{a_i}|Com_{a_i}|Rat_{a_i}|E_{a_i}|GRat_{KID-1}|\\ GRat_{KID}|\sigma_{h,*} \tag{1}$$

   In the REV_{a_i}, $KID = a_i$ is the unique identity of a review, Com_{a_i} is the comment of the user with pseudonym $ID_{h,*}$, $Rat_{h,*}$ is the score for the service of the user, $E_{h,*}$ is the entangled message of t other reviews, $GRat_{KID}$ is the general rating of the SRS provided by the vendor. When review REV_{a_i} is submitted to the vendor, $\sigma_{h,*}$is the signature of the review content from a user of the group, which is used to verify the authenticity of the review.

$$\sigma_{h,*} = Sign_{sk_V}(KID|ID_{h,*}|ID_V|TK_{h,*}|s_{h,*}|T_{h,*}|Com_{h,*}|Rat_{h,*}|E_{h,*}|\\ GRat_{KID-1}|GRat_{KID}) \tag{2}$$

   For example, $GRat$ is the average of all review Rats in the system which is used for rating a service in different aspects, and the value ot $GRat_{KID}$ is

$$GRat_{KID} = \frac{GRat_{KID-1}(KID-1) + Rat_{KID}}{KID}, \tag{3}$$

   when all the general ratings are correctly computed.
3. When u_j receives the t reviews according to the seed $s_{h,j}$, it will verify the correctness of the $t+1$ reviews. If they pass the validity test, then u_j computes $e_{a_i} = H(REV_{a_i})(1 \leq i \leq t)$ and entangled data $E_{h,j} = \oplus_{i=1}^{t} e_{a_i}$ and then generates its review REV_{N+1} as show in (2):

$$REV_{N+1} = N+1|ID_{h,j}|ID_V|TK_{N+1}|s_{N+1}|T_{N+1}|Com_{N+1}|Rat_{N+1}|E_{N+1}|\\ GRat_N|GRat_{N+1}|\sigma_{N+1}. \tag{4}$$

In REV_{N+1}, we have $Tk_{N+1} = TK_{h,j}$ and $s_{N+1} = s_{h,j}$ as sent in message $Msg_{h,j}$.

Step3: In the indirect seed submission phase, the message $Msg_{h,j}$ is sent to MC, which will verify the validity of the message and forward $Msg_{h,j}$ to the vendor V. Since the mobile is considered as a trusted part in our network model, the verification of t random reviews as shown in Step 2.2 and the generation of the entangled data as shown in Step2.3 are conducted by MC instead of u_j. After generating $E_{h,j}$, MC will designate a valid user u_* of the MC to send $E_{h,j}$ to u_j in a message $Msg_{u_*} = ID_{u,*}|ID_{u,j}|s_{N+1}|T_{u,*}|E_{N+1}|GRat_N|\sigma_{u,j}$. Then, the only thing u_j needs to do is to verify the integrity of $E_{h,j}$ and generate its review $Msg_{h,j}$.

Review Submission.

u_j submits its review $Msg_{h,j}$ to the vendor V. When V receives the review, it will firstly verify the validity of $Msg_{h,j}$ and $TK_{h,j}$. Then, it assigns a unique identity KID for $Msg_{h,j}$ and computes the general rating $Grat$ of the service according to the review of u_j. If the review is legitimate, u_j will store and publish the review in its local repository. Review submission may be conducted directly between the vendor and users when they are in the communication range of each other. However, when the vendor is out of a user's communication range, the MC will cooperate with users and help them to verify the authenticity of vendor's activity and forward the review of users.

4.3 Efficient and Privacy Preserve M-SRSs

Notice that it is important to improve the efficiency of the system and protect the privacy of users in our M-SRS. The identity based aggregate signature and pseudonyms could be adopted.

Efficient M-SRS based on aggregate signature(EM-SRS). The detail of EM-SRS will be instantiated as bellow.

Setup: The Private Key Generator (PKG) generates parameters and keys essentially as bellow. Specifically, the TA:

1. generates groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q and an admissible pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$;
2. chooses an arbitrary generator $P \in \mathbb{G}_1$;
3. picks a random $s \in \mathbb{Z}/q\mathbb{Z}$ and sets $Q = sP$;
4. chooses a cryptographic hash functions $H_1, H_2 : \{0,1\}^* \to \mathbb{G}_1$ and $H_3 : \{0,1\}^* \to \mathbb{Z}/q\mathbb{Z}$.

The published system parameters are $params = (\mathbb{G}_1, \mathbb{G}_2, \hat{e}, P, Q, H_1, H_2, H_3)$. The root PKG's secret is $s \in \mathbb{Z}/q\mathbb{Z}$.

User Private key generation: The user u_j with identity ID_j receives from the TA the secret key $sk_j = sP_{j,i}$ for $i \in \{0,1\}$, where $P_{j,i} = H_1(ID_j, i) \in \mathbb{G}_1$.

Individual Signing: The vendor chooses a random string Str that has never been used before and publishes it to its group members. When u_j wants to sign the review content $\alpha_j = ID_{h,j}|TK_{h,j}|s_{h,j}|T_{h,j}|Com_{h,j}|Rat_{h,j}|E_{h,j}$, ID_j will:

1. computes $P_{Str} = H_2(Str) \in \mathbb{G}_1$;

2. computes $c_j = H_3(m_j, ID_j, Str) \in \mathbb{Z}/q\mathbb{Z}$;
3. generates a random number $r_j \in \mathbb{Z}/q\mathbb{Z}$;
4. computes the signature $\sigma_j = (Str, S'_j, T'_j)$, where $S'_j = r_j P_{Str} + sP_{j,0} + c_j sP_{j,1}$ and $T'_j = r_j P$.

When a user requires t random reviews from the vendor, it could conduct the signature aggregation as follows.

Aggregation: Every user in the group can aggregate a collection of individual signatures that uses the same string Str. For example, individual signatures (Str, S'_j, T'_j) for $1 \leq j \leq t$ can be aggregated into $\sigma = (Str, S_t, T_t)$, where $S_t = \sum_{j=1}^{t} S'_j$ and $T_t = \sum_{j=1}^{t} T'_j$.

Verification: Let σ be the identity-based aggregate signature. The user could check the validity of the t reviews from the vendor, as shown in the following formula.

$$\hat{e}(S_t, P) \stackrel{?}{=} \hat{e}(T_t, P_{Str})\hat{e}(Q, \sum_{j=1}^{t} P_{i,0} + \sum_{j=1}^{t} c_j P_{j,1}) \tag{5}$$

Privacy preserve M-SRS based on pseudonyms (PPM-SRS). In the identity based pseudonyms, pseudonyms can be used for vendors and other users to verify the message of the user. Thus, if the reviews are associated with pseudonyms, the vendors and other users are able to check the authenticity of the reviews and TA is able to trace the reviews generated by their group members.

5 Security Analysis

In this section, we show that M-SRS is secure with respect to the following security analysis.

5.1 Security Against Selective Review Delete Attack

In the situation that some users synchronously submit their reviews, they could entangle the reviews of other users and submit the entangled review IDs for other user to verify.

The following theorem indicates that the selective review delete attack can be detected with high probability.

Theorem 1. *The vendor is able to delete reviews without being detected with high probability if and only if the reviews are not entangled by other reviews stored in the SRS.*

Proof. Suppose that the vendor deletes a set of reviews in the SRS and there are still a set of valid reviews SET containing the entangled data of those deleted reviews stored in the system. Then, since the signature scheme adopted in our scheme is secure, a malicious vendor could not modify the content of the reviews stored in the system. The malicious activity of the vendor will be detected by the

users who submit a review that requires to check the correctness of the reviews in SET. The probability that some user detects the selective review delete relies on the probability that a user needs to generate entangled data using a reviews in SET. According to the more detailed detection probability of selective review delete attack below, even a small fraction of reviews is deleted by the vendor, the users will be able to detect this malicious behaviour with high probability when those deleted reviews are entangled by some other reviews stored in the system. It means that a malicious vendor needs to delete all the entangled reviews in the system to avoid being detected, and this completes the proof.

We now analyse the probabilistic guarantees offered by our scheme. According to the construction of our scheme, each review $REV_i (1 \leq i \leq N)$ stores an entangled data E_i generated from t random previous reviews according to a random seed s_i. Even if one of the t review is deleted or modified, a user would not be able to generate a validate entangled data E_i' with $E_i' = E_i$. Therefore, we assume that there are N reviews stored in the SRS of a vendor. The vendor V deletes c out of N reviews in its SRS. Let t be the number of different reviews a user U asks for entangling in its review. Let X be a discrete random variable that is defined to be the number of reviews chosen by U that matches the reviews that deleted by the vendor. We compute P_X, the probability that at least one of the reviews picked by the user matches one of the reviews deleted by the vendor. We have:

$$P_X = P\{X \geq 1\} = 1 - P\{X = 0\} = 1 - \frac{n-c}{n} \cdot \ldots \cdot \frac{n-t+1-c}{n-t-1} \tag{6}$$

Because we have $\frac{n-i-c}{n-i} \geq \frac{n-i-1-c}{n-i-1}$. It follows that:

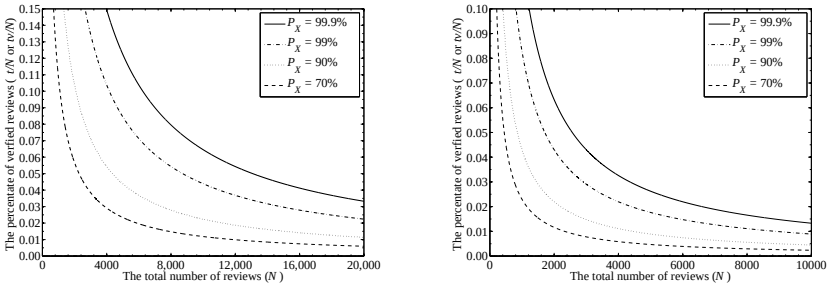
$$1 - (\frac{n-c}{n})^t \leq P_X \leq 1 - (\frac{n-t-1-c}{n-c-1})^t \tag{7}$$

P_X indicates the probability that, if V deletes c blocks of the file, then U will detect vendor misbehaviour after a review submission in which it asks proof for t blocks. Fig. 1 plots P_X for different values of N, t, c. When c is a fraction of the file, U can detect vendor misbehaviour with a certain probability by asking proof for a constant amount of reviews, independently of the total number of file blocks: e.g., if $c = 1\%$ of N, then u asks for 460 blocks and 300 blocks in order to achieve P_X of at least 99% and 95%, respectively.

We assume that P_Y is the probability that at least one of the reviews picked by v different users matches one of the reviews deleted by the vendor. Also, we assume that the vt randomly selected reviews are different from each other. Then, we have:

$$1 - (\frac{n-c}{n})^{tv} \leq P_Y \leq 1 - (\frac{n-t-1-c}{n-c-1})^{tv} \tag{8}$$

It is obvious that, the communication and computation overhead of users (in M-SRS) and the mobile cloudlet (in EM-SRS) increase with t. Formula (8) shows



(a) $c/N = 1\%$ (b) $c/N = 5\%$

Fig. 1. The detection probability of review deletion

The figures show that our scheme could provide a very high selective review deletion attack detection probability, when the review number is significantly large and only a small fraction of reviews are deleted by the malicious vendor.

that the high detection probability could be realized according to the contribution of different users. Meanwhile, assuming that the vt reviews are different, we could also detect selective review deletion attack with high probability as show in Fig. 1.

5.2 General Review Results Security

According to the above analysis, our scheme is secure against the review modification, injection and deletion attack. Therefore, the security of the general review results of our scheme can be analyzed through the following two aspects when a user provides a review with wrong general review results.

First, when a user provides a wrong negative review, the vendor will detect the malicious of the user and then reject the review or ask the user to calculate a new review with right general review results.

Second, when a user provides a wrong positive review, a selfish vendor may accept and store the reviews in its system. However, the general review results are public verifiable, the new review submitter and the users in the mobile cloudlet will find the malicious activity of the vendor. The probability for users to detect this malicious activity of vendor is the same as the probability analysis shown in section 5.1.

6 Conclusion

The mobile cloudlet assisted SRS is introduced in this paper, in which the review entanglement and some identity based signature schemes are adopted to guarantee the security and improve the efficiency. The solutions provide a verification of the vendor's malicious activity with high probability for the whole reviews in the SRS. Also, it shows that our efficient schemes will significantly

reduce the computational and communicational overhead of users by adopting mobile cloudlet.

Acknowledgement

This work is supported by the National Natural Science Foundation of China (Nos. 61272455 and 61100224), Doctoral Fund of Ministry of Education of China,Program for New Century Excellent Talents in University, and China 111 Project (No. B08038).

References

1. Aspnes, J., et al.: A critical evaluation of location based services and their potential. Journal of Location Based Services 1(1), 5–45 (2007)
2. Aspnes, J., et al.: Towards a theory of data entanglement. Theoretical Computer Science 389(1-2), 26–43 (2007)
3. Dhar, S., Varshney, U.: Challenges and business models for mobile location-based services and advertising. Communications of the ACM 54(5), 121–128 (2011)
4. Dinh, H., et al.: A survey of mobile cloud computing: architecture, applications, and approaches. Wireless Communications and Mobile Computing 1(1), 1–25 (2011)
5. Fernando, N., Loke, S., Rahayu, W.: Mobile cloud computing: a survey. Future Generation Computer Systems 29(1), 84–106 (2013)
6. Gentry, C., Ramzan, Z.: Identity-based aggregate signatures. In: Public Key Cryptography (PKC'06). Lecture Notes in Computer Science, Springer-Verlag, NY, USA (2006)
7. Ghinita, G., et al.: Private queries in location based services: anonymizers are not necessary. In: Proc. ACM International Conference on Management of data (SIGMOD'08). pp. 121–132. NY, USA (Apr 2008)
8. Hengartner, U.: Location privacy based on trusted computing and secure logging. In: Proc. ACM International Conference on Security and privacy in communication netowrks (SecureComm'08). pp. 22–25. Waterloo, Canada (Sep 2008)
9. Khan, A., et al.: Towards secure mobile cloud computing: A survey. Future Generation Computer Systems 29(5), 1278–1299 (2013)
10. Liang, X., et al.: Seer: A secure and efficient service review system for service-oriented mobile social networks. In: Proc. IEEE International Conference on Distributed Computing Systems (ICDCS'12). pp. 647–656. Macau, China (Jun 2012)
11. Pan, X., Xu, J., Meng, X.: Protecting location privacy against location-dependent attacks in mobile services. IEEE Transactions on Knowledge and Data Engineering 24(8), 1506–1519 (2011)
12. Satyanarayanan, M., et al.: The case for vm-based cloudlets in mobile computing. IEEE Pervasive Computing 8(4), 14–23 (2009)
13. Tsai, H., Chen, T., Chu, C.: Service discovery in mobile ad hoc networks based on grid. IEEE Transactions on Vehicular Technology 58(3), 1528–1545 (2009)
14. Zhang, Y., Wu, Z., Trappe, W.: Adaptive location-oriented content delivery in delay-sensitive pervasive applications. IEEE Transactions on Mobile Computing 10(3), 362–376 (2011)
15. Zhu, Z., Cao, G.: Towards privacy-preserving and colluding-resistance in location proof updating system. IEEE Transactions on Mobile Computing 12(1), 51–64 (2011)