A Survey on Enhancing Security for Mobile Advertising and Billing Information

S. Princy Rachel[1] A.H.Ragamathunisa Begam[2]
[1]P.G. Scholar [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Velammal Engineering College, Chennai, India

Abstract— Mobile devices get more involved as media delivery platforms; the worth of advertising on these devices becomes significant. Many systems have been developed to make use of this opportunity. In existing system, the peers among the group will request directly for advertisements to ad-server which leads to lack of privacy in the system. Because of this act of the peers, the other peers among the group can easily access the request of the particular peer which is not a valid process on ad-server. To overcome this, we propose a model to enhance the security process of previous system and to reduce the communication cost. We developed three roles: Service Provider, Content Provider, and Mobile Peers. Service provider provides the advertisement to Ad-Server. Ad-server distributes the advertisements to the Content Provider. Mobile peers (user) install third party application. The peer group formation starts when a peer broadcasts an ad announcement. We used three different algorithms to overcome the problem of existing system, we generate key signature using HMAC algorithm, the data transformation between the peers and the ad-server process is done securely using Base64 algorithm and the energy efficiency in the primary peer is increased using RSA algorithm. We introduce the concept of re-encryption process using the intermediate peer among the group of peers to enhance the security so that the peer's id is hidden from the ad-server as well as the primary peer to avoid unauthorized process.

Key words: Network Privacy, Mobile Advertising, Billing Informations, Collaboration, Mobile Devices, Mobile Computing

I. INTRODUCTION

Mobile advertising is a rapidly developing sector which provides brands, agencies and marketers the opportunity to connect with consumers. Users spend significant time browsing the different multimedia and gamming and get exposed to ads. The Customized advertisement matches with user preferences with product to achieve better customer satisfaction. these devices now come with Wi-Fi and 3G, meaning they can be reached virtually everywhere. Add to this GPS capability and computing user preferences, and a new level of targeted advertising can be attained.

We propose a system for Mobile advertising relies on content providers like applications and WebPages to deliver ads to users. Service providers register ads to an ad-server, which delivers them to users through content providers who usually subscribe to host ads for profit making. When a user accesses an application subscribed to an ad-server, the application requests an ad from the server with the user location and id. The server then checks based on the id the interests of the user through an online profile, and delivers targeted ads that refer to service providers in the vicinity of the user which are relevant to his interests. For example, a user in downtown San Francisco interested in pizza will get an ad for pizzerias within that location. After the user clicks the delivered ad, a click Report is sent to the ad-server for billing purposes.

The present advertising model relies in the following classes of threats:

- Direct advertisement request in ad-server leads to lack of privacy.
- Expired ads of the user get received during shuffling process leads to cause of multiple participation.
- Algorithm used for encrypt and decrypt the message is not satisfactory.
- Overlapping of data occurs during multiple participation of expired ads.

II. BACKGROUND AND RELATED WORKS

To frame the problem, we describe how mobile advertising currently works and how the present scenario in advertisements leads to the privacy and security threats from malicious advertising and vulnerable advertising networks.

A. Related Works

Concurrent with this work, several other researches have explained about mobile advertisement services which have explained as, [1]A system for delivering context, location, time, and preference-aware advertisements to mobiles. The main adversary in our model is the server distributing the ads, which is trying to identify users and track them, and to a lesser extent, other peers in the wireless network.

Here, Direct advertisement request in ad-server leads to lack of privacy. Algorithm used for encrypt and decrypt the message is not satisfactory. [3] A Distributed mechanism for users to augment their profile in a way that confuses the user-item connection to an un-trusted server, with minimum loss on the accuracy of the recommender system. By using the method called Netflix prize dataset.[4] provides a tool to separate the privilege given to advertisers in android from application requesting ads. Based on the notion of applications are granted the privilege of accessing the user's preferences. [6] Rapid expansion of wireless technologies has provided a platform to support intelligent systems in the domain of mobile marketing.

Personalized and context-aware advertisements to fulfill customer needs.[2] MobiAd would perform a range of data mining tasks in order to maintain an interest profile on the user's phone, and use the infrastructure network to download and display relevant ads.[8] The system was designed to constantly deliver advertisements and information to wandering customers according to their location and previous visits. It is based on mobile advertising in a mall based on a hybrid system using a bluetooth system. [10] operates by grouping users into a

large and geographically diverse group (crowd) that collectively issues requests on behalf of its members. It uses degrees of anonymity as an important tool for describing and proving anonymity properties.

III. PROPOSED SYSTEM

Mobile advertising relies on content providers like applications and WebPages to deliver ads to users. Service providers register ads to an ad-server, which delivers them to users through content providers. When a user accesses an application subscribed to an ad-server, the application requests an ad from the server with the user location and id. The server then checks user id and delivers targeted ads that refer to service providers in the vicinity of the user which are relevant to their interests.

The challenges to be focused by adding the following significant contributions:

- Enhanced security by introducing an intermediate peer among the group.
- Standard algorithm is used for encryption and decryption process for security purpose.
- An aggregation scheme and a piggyback method that protects the system from multiple participation of expired ads.

IV. ARCHITECTURE AND DESIGN

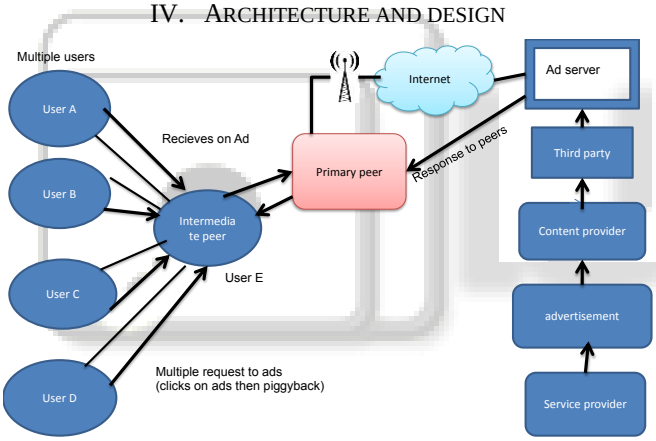

Fig. 1: Overall System Component

A. Architecture Design Elaboration:

The proposed system is for users to aggregate user's interests when requesting advertisements to hide user identities from the ad server. We developed three roles: Service Provider, Content Provider, and Mobile Peers. Service provider provides the advertisement to Ad-Server. Ad-server distributes the advertisements to the Content Provider. Mobile peers (user) install third party application. As in fig1.1, The peer (mobile users) group formation starts when a peer broadcasts an ad announcement. Peers who hear the message and need ads will reply with an acknowledgement and join the group.

After choosing the primary peer, all participants in the group generate interests and encrypt these interests along with billing reports, which capture their clicks on previous ads, using the primary peer's public key. With this process, peers hide their data from each other. Next, each peer randomly chooses another peer which is called an intermediate peer in the group, it is chosen by referring higher priority. The intermediate peer will encrypts the encrypted message with his public key, before broadcasting it. With this mechanism, only that particular peer will be able to decrypt this message before transmitting it to the primary peer. As the primary peer receives these packets, it decrypts them using its private key, and aggregates them to be sent to the server. When the ad server receives the interests, it replies with ads to the primary peer, who will then broadcast them to the group.

V. PROPOSED DESIGN MODEL

The main aim of this project is to provide user's with personalized advertisements without affecting privacy from Ad-server. To provide benefits to the mobile users as well as Content Providers for viewing and disseminating advertisements respectively. Reduce the communication cost by piggybacking. To achieve this, few modules have been developed.

A. Post Advertisement

In this module, Service Provider and Content Provider have to register their details with the ad-server. After successful registration, details are stored in database. Service Provider login with their credentials and then post an advertisement to Ad-server with image, tags and benefits per clicks (both to content provider and user). Ad-server view the advertisements posted by the service provider and allocate to the content provider.

B. Peer Formation in Network:

In this module, Peers are created based on coverage. Authority will generate public keys and private key for all peers using RSA algorithm. Public keys are distributed to all peers within coverage. The group formation starts when a peer broadcasts an ad announcement. Peers who receive the message and need ads will reply with an acknowledgement and join the group. Peer who one is acknowledged first then we selects that peer as primary peer.

C. Request Aggregation on Primary Peer:

Peer sends the advertisement request to server through primary peer and random choosing peer. Peer who is selected as a random peer will encrypt the advertisement using public key and forward to primary peer, then primary peer verifies the signature and then re-encrypts the advertisement. This re-encryption ensures the protection of data privacy and user privacy. Finally, after the primary peer receives all requests, it aggregates them and sends them to the ad server, and then waits for a reply. The ad server process the requests from the primary peer by finding the ads with metadata offering the best match to the tags contained in the message and replies back with the corresponding ads to the primary peer.

D. Billing Process and Piggybacking:

Primary peer broadcast the advertisement to the peers within the coverage; only the requested mobile peers will receive the advertisement. Sybil attack could occur if a certain peer generates large amounts of "fake" click reports to charge service providers more. To rectify the Sybil attack if the peer generates a large amount of click reports ad-server will considered it as a one click. Piggybacking literally refers to carrying someone on one's back or shoulders. It may also refer to: Piggyback (transportation), something that is riding

on the back of something else. Piggybacking (security), when an authorized person allows (intentionally or unintentionally) others to pass through a secure door. The ad server should be able to reliably bill service providers for the offered advertising services. Service provider will credit amount to the content provider and the peer. The billing is also raised from the user by using piggybacking when the next advertisement request is triggered from the user mobile device.

VI. CONCLUSION

We developed a privacy preserving mobile advertising system, where we considered a UN trusted ad-server and users who do not trust each other with their interest information. The architecture relies on cooperative behavior among nodes to request ads and distribute them to each other, and to implement a mixing algorithm to hide the interests of users from each other and their identities from the server.

REFERENCES

[1] H. Artail, Senior Member, IEEE and R. Farhat, "A Privacy-Preserving Framework for Managing Mobile Ad Requests and Billing Information," IEEE Transaction on Mobile Computiung , Vol. 14, No. 8, August 2015, pp. 1560-1572.
[2] H. Haddadi, P. Hui, and I. Brown, "MobiAd: Private and scalable mobile advertising," in Proc. 5th ACM Int. Workshop Mobility Evolving Internet Archit., 2010, pp. 33–38.
[3] R. Shokri, P. Pedarsani, G. Theodorakopoulos, and J. Hubaux, "Preserving privacy in collaborative filtering through distributed aggregation of offline profiles," in Proc. 3rd ACM Conf. Recommender Syst., 2009, pp. 157–164.
[4] P. Pearce, A. Felt, G. Nunez, and D. Wagner, "AdDroid: Privilege separation for applications and advertisers in android," in Proc. 7th ACM Symp. Inf., Comput. Commun. Security, Seoul, Korea, May 2012, pp. 4–5.
[5] X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: A secure and privacy preserving protocol for vehicular communications," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, Nov. 2007.
[6] B. R. Prasad Babu, Jaya Kumar, and V. R. Bharatesh, "A intelligent android Mobile based real time Ads tracking System," IEEE International Journal of Advanced Research , Comput. Commun. Eng., Vol. 3, Issue 6, Jun. 2014.
[7] M. J. Freedman and R. Morris, "Tarzan: A peer-to-peer anonymizing network layer," in Proc. 9th ACM Conf. Comput. Commun. Security, 2002, pp. 193–206.
[8] J. Sanchez, J. Cano, C. Calafate, and P. Manzoni, "BlueMall: A bluetooth-based advertisement system for commercial areas," in Proc. 3rd ACM Workshop Perform. Monitoring Meas. Heterogeneous Wireless Wired Netw., 2008, pp. 17–22.
[9] A. Narayanan and V. Shmatikov, "Robust de-anonymization of large sparse datasets," in Proc. IEEE Symp. Security Privacy, 2008, pp. 111–125.
[10] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for web transactions," ACM Trans. Inf. Syst. Security, vol. 1, pp. 66–92, 1998.

