A Conceptual Framework for Mobile-Ad Management using Caching and Relevance Mapping with Privacy Protection

[1]S.Balaji, [2]M.Charumathi, [3]M.Hindu, [4]G.Navaneetha
[1]Assistant Professor, [234]UG Student,
Department of Computer Science and Engineering
GRT Institute of Engineering and Technology, TamilNadu, India.

Abstract

Mobile advertisements in smart phones and gadgets have increased. But the privacy of mobile users is under annoyance. The proposed system is to aggregate user's interests when requesting advertisements to hide user identities from the ad server. 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. When a node is interested in an ad, it forms a group of nearby nodes seeking ads and willing to cooperate to achieve privacy. 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 request. The relevance mapping is done in the ad-server and associated as requests are aggregated. Another mechanism is proposed to implement the billing process without disclosing user identities using piggybacking.

Keywords: *peer, primary peer, content provider, service provider, piggybacking.*

I. INTRODUCTION

Advertising on smart devices as become momentous as people get more involved on media delivery platforms. Advertisement through mobile phones is known as mobile advertising. Advertisements are sent to the smart phones are delivered through the applications installed in the mobile devices and through the Web sites they visited. By Mobile Demand sites also the advertisements can be purchased. Now-a-days billion of people were using smart phones, they are exposed to many media platforms, and there is a huge market for advertising. As the mobile app users are increased the demand for related advertisements also increased. The smart phone users spend more time on browsing the different multimedia and games, these makes them more exposed to advertisements. As the mobile phones come with Wi-Fi and 3G, the user can search anything from anywhere.

The mobile phones also have GPS technique through which the user locations are also identified. Personalized advertisement is to provide user interested advertisement this will provide higher chances of succeeding in capturing these users' attention and achieving better customer satisfaction, consequently increasing the profitability of advertisements. Advertisements through mobile devices improves the communication with customers, this may cause privacy violations. Considering that marketing through mobile devices is rapidly increasing. Using mobile advertisements the product marketers directly deal with the consumers.

Gartner predicts the mobile advertisement market to grow to $13.5 billion in 2015. Mobile advertisements are delivered through advertising libraries which are embedded in the application at compile time. These libraries generally use an embedded web browser, Android's Web View, to display the advertisements and handle user interaction. These Web Views are subject to many of the same security concerns that impact other dated web browsers. These libraries then handle the work of requesting the advertisement from a central server, displaying it to the user, and tracking the user's interaction with the advertisement. Individuals are much more attached to their mobile devices than to their laptops and personal computer. They store all their sensitive and personal information in their mobile devices. Successful and accurate profiling and personalization of advertisements will depend strongly on ad networks assuaging consumer's privacy concerns over targeted advertisements. As the effectiveness of advertising largely depends on the relevance between the delivered advertisements and user's interests, a popular paradigm for current online advertising system is targeted advertising, where advertisers appoint an ad broker to deliver advertisements to potentially interested users by analyzing users' online profiles or behaviors. Targeted advertising is beneficial to both advertisers and users: advertisers can gain higher revenue by advertising to users with a strong potential to purchase, and the users in turn receive more pertinent and useful ads that match their preferences and interests.

Due to the increased effectiveness and benefits, a number of advertisers around the world have already turned to online targeted advertising systems. To provide targeted advertisements to the users the Ad-Server track the user's personal details, location, and id. To avoid this, a system is proposed that forms a group among the mobile nodes which are interested on advertisement. The advertisement request from each mobile node is encrypted and shuffled using shuffling mechanism, then sent to the primary peer. The primary peer sends the request to the Ad-Server and gets advertisement from the Ad-Server. Then it delivers advertisement to the mobile nodes in the group. Through this process the user identities are hided from the Ad-Server.

II. RELATED WORK

[1] As the increasing number of smart phones with internet facilities mobile marketing increases quickly. Mobile advertising enhances communication with consumers. These mobile advertisements sent by the Ad-server causes privacy violations, they access the user's personal profile to get their interest. To avoid this Privacy Preserving Model for Personalized Mobile Marketing, is proposed that can protect both user's preferences and location privacy while supporting personalization in mobile marketing, a prototype is implemented to apply this system in practice. But this prototype cannot manage large volume of queries.

[2] MobiAd is introduced to 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 and reports the clicks via a Delay Tolerant Networking (DTN) protocol. MobiAd provides privacy concerns on mobile phones, in addition to the scalable local ad download and privacy-aware DTN-based click report dissemination methods. MobiAd prototype is not applicable for Apple iPhone, Google Android and Microsoft Windows mobile platforms.

[3] The proposed system is for delivering location and preference-aware advertisements to mobiles with a novel architecture to preserve privacy. When the need for advertisements arises, the node will form a group of nearby nodes seeking ads and will cooperate to achieve privacy. Peers combine their interests using a "shuffling" mechanism in an ad-hoc network and send them through a "primary peer" to the ad server. Another mechanism is implemented to protect from fraud clicks and Sybil attacks is called robust and anonymous billing system. It is found that caching ads increases the privacy within the system but causes increased costs on the primary peers.

[4] As the smart phone user's are increasing, online advertising also increased, which provides personalized advertisement by accessing the user profile. MobiAd includes protocols for scalable local advertisement download and privacy-aware click report dissemination. Delay Tolerant Networking (DTN) protocol is the security mechanism used to find fraud clicks and to preserve the privacy and anonymity of the user. Bluff ads is a simple detection mechanism, which have a comfort factor of decreasing the user's negative perceptions by reducing the number of accurately targeted advertisements. This Bluff advertisement cannot provide large advertising services.

[5] AdSplit is an extended Android to allow an application and its advertising to run as separate processes, under separate user-ids, eliminating the need for apps to request permissions on behalf of their advertising libraries, and providing services to validate the legitimacy of clicks, locally. AdSplit automatically recompiles apps to extract their ad services. AdSplit also supports a system resource that allows ads to display their content in an embedded HTML widget, without requiring any native code. The HTML security model and smart phone security model are not merged. In this system, a third party review process is needed to quickly update the applications.

[6] The PrivAd an online advertising system designed to be faster and more private to fill the needs of targeted advertisement. Privad occupies a point in the design space that strikes a balance between privacy and practical considerations. PrivAd substantially provide better privacy while fitting into today's advertising business model. PrivAd components are not more effective to do profiling, to run auctions, the bait approach to click-fraud and privacy from the advertiser.

[7] An Empirical method is used to collect database of over 225,000 ads on 32 simulated devices hosting one of three distinct user profiles. The collected data are then analyzed to know how the ads are targeted by correlating ads to potential targeting profiles using Bayes' rule and Pearson's chi squared test. The empirical method preserves the user profiles to become ever more accurate and personal, making the distinction between personal identification and a theoretically anonymous profile more and more difficult to sustain. But it cannot collect large scale of data sets.

[8] Privacy aware framework to promote targeted advertisement is proposed in which the Ad-broker who provides personalized advertisements to the users, sits between advertisers and users for targeted advertising and provides certain amount of compensation to incentivize users to click ads that are interesting yet sensitive to them. The ad broker and the users are analyzed by formulating the problem as a three-stage game, in which a unique Nash Equilibrium is achieved. This system analyses the

players' behaviors for the scenarios of independent advertisers and competing advertisers.

[9] MAdScope is a novel tool used to provide targeted advertisement to the mobile users that can quickly harvest the advertisement from a large collection of apps, systematically probe an ad network to characterize its targeting mechanism and emulate user profiles of specific preferences and interests to study behavioral targeting. API is to provide lot of information to ad network, it is provided by the app developer. The MAdScope tool cannot provide targeted in-browser advertisements.

[10] In order to provide personalized advertisement to the user the Ad server accesses the user's personal profile. The proposed system explains how much of the user's interest and demographic information such as gender, parental status is known to the Ad-network on the mobile platform. This system cannot store the advertisement data for long period of time.

[11] AdFisher is an automated tool proposed in this system that explores how user behaviors, Google's ads and Ad Settings interact. AdFisher is used to find that the Ad Settings was opaque about some features of a user's profile, that it does provide some choice on ads, and that these choices can lead to seemingly discriminatory ads. AdFisher tool provides advertisement based on genders. Males were shown ads encouraging the seeking of coaching services for high paying jobs more than females. This system is not applicable for advertising systems like Facebook, Bing, or Gmail.

[12] ObliviAd which is a secure architecture for privacy preserving Online Behavioral Advertising (OBA) is proposed. ObliviAd does not assume any trusted third-party and provides brokers an economical alternative that preserves the privacy of users without hampering the precision of ads selection. This system utilizes PIR technology which implements secure coprocessor and an efficient ORAM construction. The proposed system formalizes two privacy goals profile privacy and profile unlinkability. It provides complete implementation of the system, comprising a browser plug-in and open-source software for brokers. Cryptographic coprocessor used in this system is more expensive, a trusted third-party module (TPM) can be implemented as alternative which is inexpensive than cryptographic coprocessor.

III. PROPOSED SYSTEM

A. Piggybacking

The main aim of the proposed system is to provide users with personalized advertisements without affecting privacy from Ad-server and to provide benefits to the mobile users as well as Content Providers for viewing and disseminating advertisements respectively. In the proposed system the communicational cost is reduced using piggybacking. 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 is (security), when an authorized person allows (intentionally or unintentionally) others to pass through a secure door.

B. Primary Peer

The proposed system is to aggregate user's interests when requesting advertisements to hide user identities from the ad server. Three roles are developed such as 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 advertisement announcement. Peers who hear the message and need advertisements will reply with an acknowledgement and join the group. Some peers cannot hear the announcement, but can still hear the broadcast of peers that have joined 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 advertisements, using the primary peer's public key. With this process, peers hide their data from each other. Next, each peer randomly chooses another peer in the group and encrypts the encrypted message with his public key, before broadcasting the advertisement request. 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 advertisements to the primary peer, who will then broadcast them to the group. Another mechanism is proposed to implement the billing process without disclosing user identities using piggybacking.

C. Advertisement Management

1) Registration

The first step in the proposed system is Post advertisements, in this module Service Provider and Content Provider have to register their details with the ad-server fig 1.1. After successful registration, details are stored in database. Service Provider login with their credentials and then posts 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.

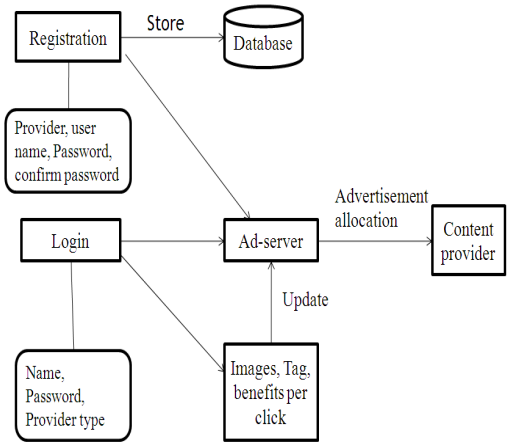

Fig 1.1 Service Provider and Content Provider Registration

2) ***Peer Formation***

The second step is Peer formation in network; here 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 advertisement announcement. Peers who receive the message and need advertisements will reply with an acknowledgement and join the group. Peer who one is acknowledged first then we selects that peer as primary peer. The peer which requests for large number advertisement is selected as Primary peer.

3) ***Request Aggregation***

The third step is 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 advertisements with metadata offering the best match to the tags contained in the message and replies back with the corresponding ads to the primary peer.

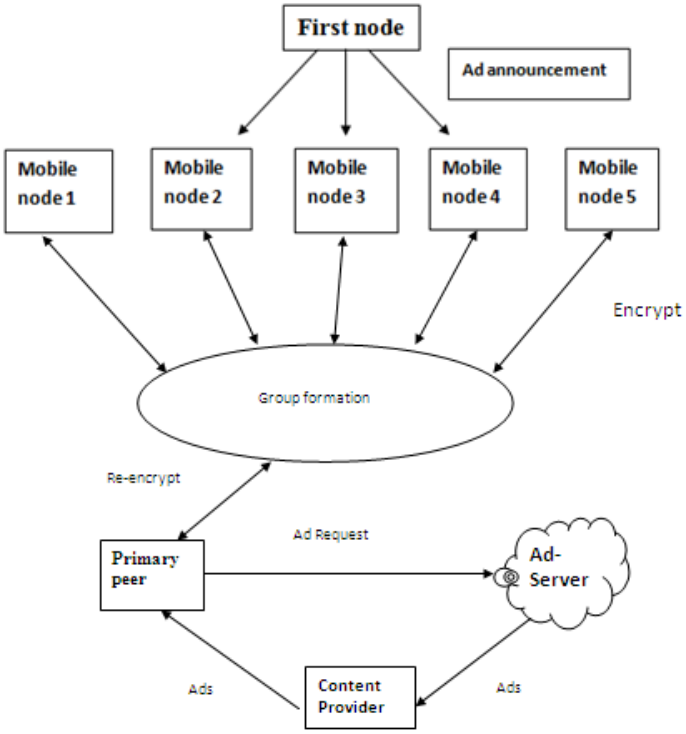

Fig 1.2 Ad Management with Primary Peer

4) ***Billing Process***

The fourth step is billing process and piggybacking, in this step the 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. 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.

The Ad-server will maintain a cache about the requests from primary peer. It will help the server when new requests are generated from the same primary peer. When the relevance of the new advertisement matches with the existing information in the cache then it is aggregated. Significantly this will reduce the efforts of processing each request and resource utilization.

In the proposed system, the key signature is developed along with each advertisement request form the mobile peer using HMAC algorithm. Using Base64 algorithm the advertisement request is sent in secured manner.

D. Relevance Identification and Caching

When the primary peer initiates and receives a ad request from the other peers it forwards the request to the ad-server. In the server, cache is verified for earlier requests from the same primary peer. If there are some earlier requests available in the cache then relevance of the new request is assessed with the existing requests.

The association identified with a rating that defines evidently the earlier requests and new request can be aggregated. If the association rating is as much as expected then a new entry is made in the cache mapping with the primary peer. The aggregation process plays a vital role in this mechanism as the association relevance should be properly represented.

Substantial increase in resource utilization and reduce processing efforts can be realized with caching technique. It will also reduce the efforts of ad-server in finding the applicable ads for a particular request since it is available in the previous request.

IV. CONCLUSION

A framework for mobile ad management with request aggregation by relevance mapping and caching in ad server has been proposed. Primary peer takes the responsibility of collecting the requests from mobile peers and forwarding it to the ad-server. The association of the request is mapped with the existing request in the cache and it is aggregated. Piggy backing helps in billing process. The proposed framework will reduce the efforts of ad-server in finding the advertisements when a new request is received and the privacy of the user is hidden from the ad-server through primary peer. It is planned to realize the framework in the cloud system in future.

REFERENCES

[1] Yuqing Sun and Guangjun Ji, "Privacy Preserving in Personalized Mobile Marketing," in proceeding of the 6th International conference, AMT 2010, Toronto.

[2] Hamed Haddadi, Pan Hui, Ian Brown, "MobiAd: Private and Scalable Mobile Advertising," in proc. 5th ACM International workshop on Mobility in the Evolving Internet Architecture, 2010, USA.

[3] Ahmed Fawaz, Ali Hojaij, Hadi Kobeissi, "PrivAd: A Privacy Preserving Targeted Mobile Advertising Architecture," thesis submitted in the American University of Brirut 2011.

[4] Hamed Haddadi, Pan Hui, Tristan Henderson and Ian Brown, "Targeted Advertising on the Handset: Privacy and Security Challenges," in HCI Doctoral Consortium, New castle, 2011, UK.

[5] Shashi Shekhar, Michael Dietz, Dan S. Wallach, "AdSplit: Separating smartphone advertising from applications," in proc. of the 21st USENIX conference on Security symposium 2012.

[6] Saikat Guha, Bin Cheng, Paul Francis, "Privad: Practical Privacy in Online Advertising," in proc. of the 8th USENIX conference on Networked systems design and implementation 2011.

[7] Theodore Book, Dan S. Wallach, "An Empirical Study of Mobile Ad Targeting," arXiv: 1502.06577v1 [cs.CR] 23 Feb 2015.

[8] Wei Wang, Linlin Yang, Yanjiao Chen, Qian Zhang, "A privacy-aware framework for targeted advertising," in the International Journal of Computer and Telecommunications Networking 2015.

[9] Suman Nath, "MAdScope: Characterizing Mobile In-App Targeted Ads," in Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services 2015.

[10] Wei Meng, Ren Ding, Simon P. Chung, Steven Han, and Wenke Lee, "The Price of Free: Privacy Leakage in Personalized Mobile In-App Ads" in proc. of the 23rd Annual Network and Distributed System Security Symposium (NDSS), February 2016.

[11] Amit Datta, Michael Carl Tschantz, and Anupam Datta, "Automated Experiments on Ad Privacy Settings," in proc. on Privacy Enhancing Technologies, 2015.

[12] Michael Backes, Aniket Kate, Matteo Maffei, and Kim Pecina, "ObliviAd: Provably Secure and Practical Online Behavioral Advertising," in proc. of the 2012 IEEE Symposium on Security and Privacy 2012.

[13] Ting Ning, Zhipeng Yang, Hongyi Wu, and Zhu Han, "Self-Interest-Driven Incentives for Ad Dissemination in Autonomous Mobile Social Networks," in proc. IEEE, 2013.

[14] Paul Barford, Igor Canadi, Darja Krushevskaja, Qiang Ma, S. Muthukrishnan, "Adscape: Harvesting and Analyzing Online Display Ads," in proc. of the 23rd international conference on World Wide Web 2014.

[15] Bin Liu, Anmol Sheth, Udi Weinsberg, Jaideep Chandrashekar, Ramesh Govindan, "AdReveal: Improving Transparency Into Online Targeted," in proc. of the twelfth ACM workshop on Hot Topics in Networks, 2013.