International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Privacy-Preserving Personlized Ad-Dissemination Based On Interest Aggregation and Piggybacking

S.Divya[1], S.Baby Shalini[2], R.Anitha[3]
[1,2,3]B.E CSE, G.K.M College Of Engineering And Technology (Affiliated to Anna University) Perungalathur, Chennai-600063.

Abstract-Advertising on mobile devices has large potential due to the very personal and intimate nature of the devices and high targeting possibilities. we introduce a piggybacking for reduce the communication cost in privacy preserving personalized ad-dissemination based on interest aggregation. We add directory servers that allow users to learn public keys. we propose a system for publish context ,location, time and preference-aware ad to mobiles with a novel architecture to preserve sequestrum. The main opponent in our model is the server distributing the advertisements, which is trying to identify users and track them, and to a lesser area, other peers in the wireless network. When a node is interested in an advertisement, then it will forms a group of nearer nodes seeking ads and willing to cooperate to achieve sequestrum. Peers combine their interests using a shuffling mechanism in an ad-hoc network and send them through a primary peer to the ad-server. In this path, preferences are masquerade to request custom ads, which are then distributed by the primary peer. Another mechanism isproposed to implementing the billing process without disclosing user identities.

Keywords: Piggybacking , preserving , ad-dissemination , opponent , sequestrum , shuffling , masquerade

I. INTRODUCTION

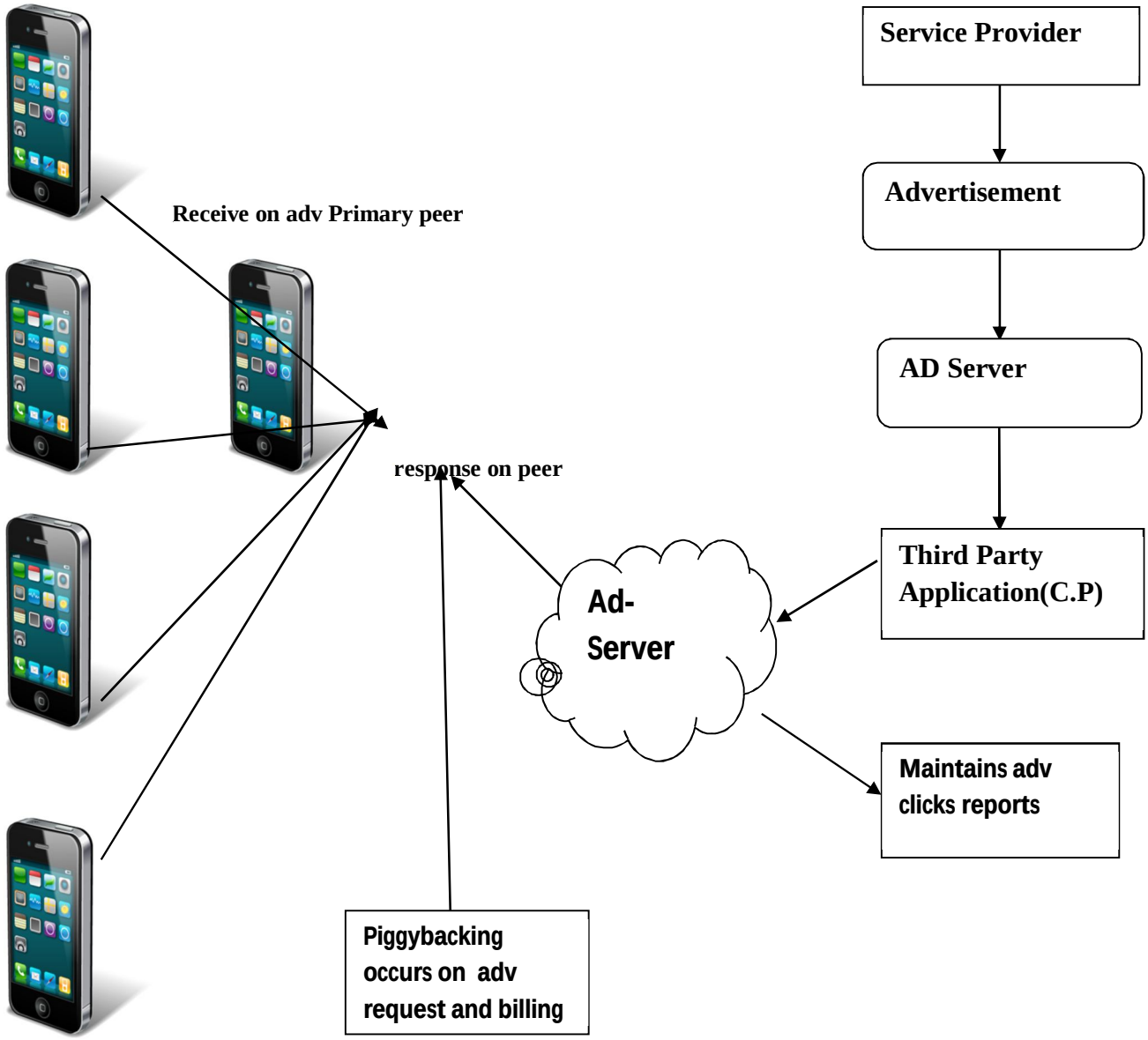
Mobile advertising has two distinct meanings: advertisements are moving from place to place, e.g. advertisements are displayed on the sides of the trucks and buses, and advertisements delivered to mobile devices, e.g. mobile phones and personal digital assistants (PDAs). Sometimes, wireless advertising is used to refer to mobile advertising. Mobile devices get more involved as media delivery platforms; the worth of advertising on these devices becomes significant. With billions of mobile users worldwide, it is indeed a potentially huge market for advertising. Moreover, considering that a decent fraction of these users own smart phones or tablets certainly expands this opportunity. These users spend significant time browsing the different multimedia and gaming capabilities of their devices, making them more exposed to ads. Also, 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. Personalized ads that can match users' preferences with products and services in their vicinities have much higher chances of succeeding in capturing these users 'attention and achieving better customer satisfaction, consequently increasing the profitability of ads. Nodes forward data on behalf of each other in mobile ad hoc networks. And we propose a system for delivering user requested advertisements and we taking into consideration context, time, and location. These are all done by summation requests and sending them via one of the users after receiving all ads, the designated user distributes the key to all the users. In which the peer(user) who selected the random peer that will provide a private key and public to all the user within the coverage. After that the user will install itself then the remaining peers will automatically receives the ads waits for reply who request to them. finally ads will be displayed to the users. For delivering location & preference aware advertisements.

II. PROBLEM FORMULATION

Personalized ads that can match users' preferences with products and services in their vicinities have much higher chances of succeeding in capturing these users' attention and achieving better customer satisfaction, consequently increasing the profitability of ads. The same aspects that make these devices great platforms for advertising also impose strict guidelines since they contain key private data, like contacts information and calendar entries. Hence, proper use and confidentiality of this data should be respected.

Volume 4 Issue III, March 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

III. ARCHITECTURE



IV. RELATED WORK

Our work preserves anonymity of mobile users submitting ad requests using techniques related to network mixes, and accordingly we give an overview of this subject first before reviewing directly related work to ours.

A. Ad-Dissemination

When the primary peer receives the reply from the ad server, it broadcasts it to the group, and filters out the ads that correspond to its own interests. Secondary peers also filter out their ads after receiving the broadcast and rebroadcast the ads to reach any remaining peers.

B. MobiAd

Advertisements target users geographically & based on their interest.Users profile is kept local & isolated from server. Ads are to be broadcasted using Multimedia Broadcast provided by UMTS.

C. MoMa System

Introduced as mobile marketing platform. Request for an ad is send to an anonymizer. Anonymizer encrypts user data & sends

request to the server. Server sends the user the specific ad.

V. METHODOLOGY

A. Existing System

Mobile advertising relies on content providers like applications and webpage's 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. The ad-server has access to all the users' personal information including their interests and location info, and thus it can easily profile users.

Timing analysis is one of them, where an adversary might know if a node is communicating with a server by correlating when messages are sent by a server and when messages are received by the node.

VI. DISADVANTAGES

Even though some are classified as real-time mixes, the majority use asymmetric cryptographic systems, where at the routing level they encrypt, or decrypt then encrypt, and then reroute, which is known to introduce large overhead.

Ad-server can track user profile information including user interest and location. And it may lead high communication cost.

Some of the proposed protocols, like ZAP, do not provide communication anonymity, while ASR uses only asymmetric cryptosystems. Many of the approaches proposed for ad-hoc networks, implicitly assume a trusted network operator and involve multiparty components for computing cryptography keys and functions.

There are several weaknesses that are associated with the proposed mix protocols in the literature. Timing analysis is one of them, where an adversary might know if a node is communicating with a server by correlating when messages are sent by a server and when messages are received by the node.

VII. PROPOSED SYSTEM

In proposed system is for users to summation user's interests when requesting advertisements to hid user identities from the ad server. We developed three roles: Service Provider, Content Provider, and Mobile Peers(user). 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 user start group formation when a user broadcasts an ad notice. Peers(users) who hear the message and need ads 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 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 in the group and encrypts the encrypted message with his public key, before broadcasting it. With this mechanism, only that particular user 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 broadcast them to the group be sent to the server. When the ad server receives the interests, it replies with ads to the primary peer, who will then

A. Advantages

A simpler overall system that allows peers to send requests any time, and does not require them to back-off for a certain time after becoming primary.

A new billing system that does not rely on a trusted third party model (server).

A new caching system that stores not only application requests but also specific requested ads.

User information's will be maintained in a privacy manner

VIII. MODULES

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

Volume 4 Issue III, March 2016
ISSN: 2321-9653

and allocate to the content provider.

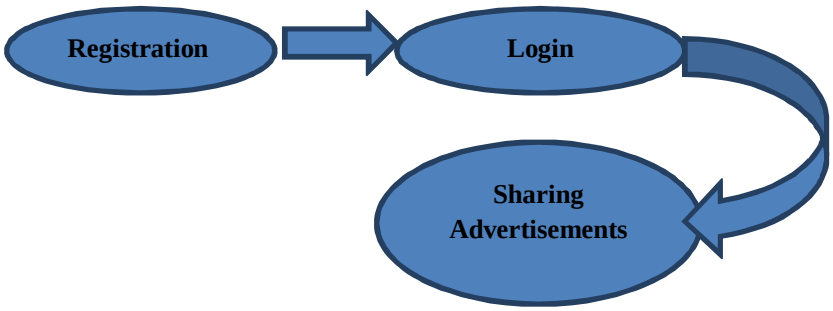
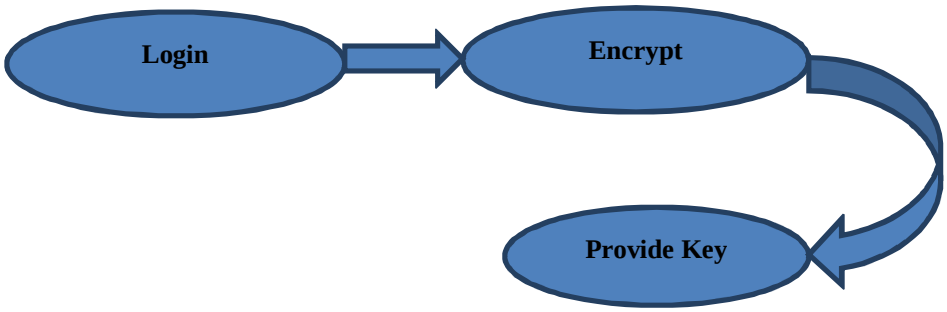


Fig: Post Advertisements

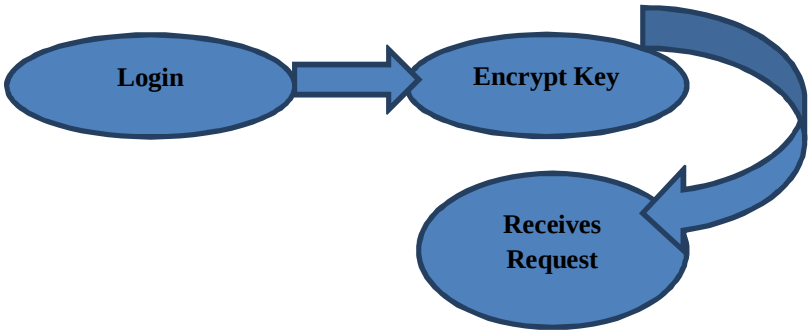
B. Peer Formation in Network

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.



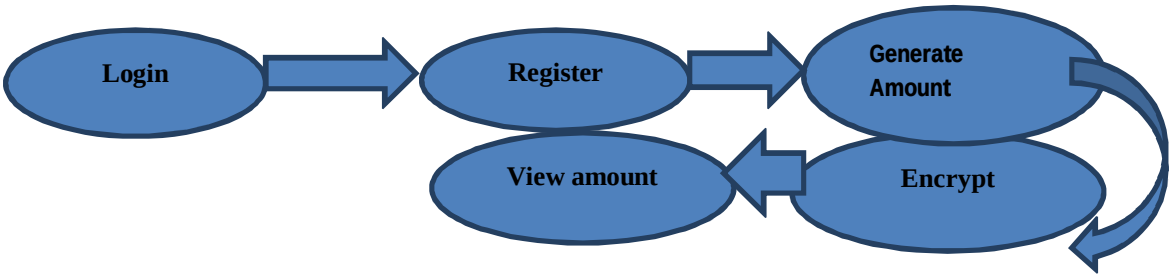
C. Request Aggregation on Primary Peer

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 .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



IX. 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.

X. ACKNOWLEDGEMENT

We would like to express our gratitude and greatest appreciation towards Prof. R ANITHA for giving us an opportunity to work under her for the project.

REFERENCES

[1] L. Aalto, N. Gothlin, J. Korhonen and T. Ojala , "Bluetooth and WAP push based location-aware mobile advertising system" , Proc. 2nd Int. Conf. Mobile Syst., Appl., Serv. , pp.49 -58 , 2004 [CrossRef]
[2] Available: http://www.knowonlineadvertising.com/ad-specs-list/, 2012.
[3] C. Andersson, M. Kohlweiss, L.A. Martucci and A. Panchenko , "A self-certified and Sybil-free framework for secure digital identity domain buildup" , Proc. 2nd IFIP WG 11.2 Int. Conf. Inf. Security Theory Practices: Smart Dev., Convergence Next Generation Netw. , pp.64 -77 , May 2008 [CrossRef]
[4] Available: https://play.google.com/store/apps/details?id=com.antutu.ABenchMark&hl=en, 2014
[5] 2010 Available: http:www.apple.comprivacy
[6] R. Bulander, M. Decker, G. Schiefer and B. Klmel , "Advertising via mobile terminals¿¿¿Delivering context sensitive and personalized advertising while guaranteeing privacy" , Proc. 2nd Int. Conf. E-Bus. Telecommun. Netw. , pp.15 -25 , 2007 [CrossRef]
[7] R. Bulander, M. Decker, G. Schiefer and B. Kolmel , "Comparison of different approaches for mobile advertising" , Proc. 2nd IEEE Int. Workshop Mobile Commerce Serv. , pp.174 -182 , 2006
[8] A. Bureau , "Internet Advertising Revenues Set First Quarter Record at 8.4 Billion" , 2012 Available: www.iab.netabout the iabrecent press releasespress release archivepress releasepr-061112
[9] H. Choi, W. Enck, J. Shin, P. D. McDaniel and T. F. La , "ASR: Anonymous and secure reporting of traffic forwarding activity in mobile ad hoc networks" , Wireless Netw. , vol. 15 , pp.525 -539 , 2009 [CrossRef]
[10] G. Danezis, R. Dingledine and N. Mathewson , "Mixminion: Design of a type III anonymous remailer protocol" , Proc. Symp. Security Priva