ACCEPTED FROM OPEN CALL

Advertising in the IoT Era: Vision and Challenges

Hidayet Aksu, Leonardo Babun, Mauro Conti, Gabriele Tolomei, and A. Selcuk Uluagac

The authors propose the architecture of an IoT advertising platform inspired by the well known business ecosystem, which traditional Internet advertising is based on. They discuss the key challenges to implement such a platform, with a special focus on issues related to architecture, advertisement content delivery, security, and privacy of the users.

Abstract

The IoT extends the idea of interconnecting computers to a plethora of different devices, collectively referred to as smart devices. These are physical items, that is, "things", such as wearable devices, home appliances, and vehicles, enriched with computational and networking capabilities. Due to the huge set of devices involved, and therefore its pervasiveness, IoT is a great platform to leverage for building new applications and services or extending existing ones. In this regard, expanding online advertising into the IoT realm is an under-investigated yet promising research direction, especially considering that the traditional Internet advertising market is already worth hundreds of billions of dollars. In this article, we first propose the architecture of an IoT advertising platform inspired by the well known business ecosystem, which the traditional Internet advertising is based on. Additionally, we discuss the key challenges to implement such a platform, with a special focus on issues related to architecture, advertisement content delivery, security, and privacy of the users.

Introduction

The Web has gained so much importance in the market economy during the last two decades because of the development of new Internet-based business models. Among those, *online advertising* is one of the most successful and profitable. Generally speaking, online advertising, also referred to as Internet advertising, leverages the Internet to deliver promotional content to end users. Already in 2011, revenues coming from online advertising in the United States alone surpassed those of cable television, and nearly exceeded those of broadcast television [1]. In addition, worldwide investment in Internet advertising reached approximately 200 billion dollars in 2016 [2] and is expected to reach 335 billion dollars by 2020 [3].

Online advertising allows web content creators and service providers, broadly referred to as *publishers*, to monetize yet provide their business for free to end users. For example, news websites or search engines can operate without charging users, as they get paid by advertisers who compete to buy dedicated slots on those web pages for showing advertisements (ads) [4–6].

The global spread of mobile devices has also been changing the original target of online advertising [7, 8]. This is indeed moving from showing traditional display advertisements (i.e., *banners*) on desktop computers to the so-called *native* advertisements impressed within app streams of smartphones and tablets [9]. More generally, the Internet advertising business will eventually extend to emerging pervasive and ubiquitous inter-connected *smart devices*, which are collectively known as the *Internet of Things* (IoT).

Enabling computational advertising in the IoT world is an under-investigated research area; nonetheless, it possibly includes many interesting opportunities and challenges. Indeed, IoT advertising would enhance traditional Internet advertising by taking advantage of three key IoT features [8]: *device diversity*, *high connectivity*, and *scalability*. IoT device diversity will enable more complex advertising strategies that truly consider *context awareness*. For example, a car driver could receive customized ads from roadside digital advertising panels based on their habits (e.g., preferred stopping locations, hotels, and restaurants). Furthermore, IoT high connectivity and scalability will allow advertising to be performed in a really dynamic environment as new smart devices are constantly joining or leaving the IoT network. Finally, different from the traditional web browser-based advertising where a limited number of user interactions occur during the day, IoT advertising might count on users interacting with the IoT environment almost 24 hours a day.

The rest of this article is organized as follows. The next section discusses the idea of IoT advertising with a use case scenario. Then we articulate key background concepts. Following that, we propose our vision of an IoT advertising landscape. In particular, we characterize the main entities involved as well as the interactions between them. We then outline the key challenges to be addressed for successfully enabling IoT advertising. Finally, we conclude in the last section.

An Example of an IoT Advertising Scenario: In-Car Advertising

Connected smart vehicles are one of the most dominant trends of the IoT industry: automakers are indeed putting a lot of effort into equipping their vehicles with an increasing set of computational sensors and devices.

With millions of smart vehicles on the road,

Digital Object Identifier:
10.1109/MCOM.2017.1700871

Hidayet Aksu, Leonardo Babun, and A. Selcuk Uluagac are with Florida International University; Mauro Conti and Gabriele Tolomei are with the University of Padua.

0163-6804/18/$25.00 © 2018 IEEE

each one carrying possibly multiple passengers, automobiles are no longer just mechanical machines used by people to move from point A to point B. Rather, they are mobile, interconnected, and complex nodes constituting a dynamic and distributed computing system. This opens up new opportunities for developers who can leverage such an environment to build novel applications and services. In particular, smart vehicles, actually passengers traveling in those vehicles, may become interesting "targets" for advertisers who want to sponsor their businesses.

Assume a family of three is traveling in their smart car, with plans to drive to a seaside destination a few hours away from their home and spend the weekend there. To do so, they rely on the GPS navigation system embedded in their car. Bob is actually driving the car; he is a 45 year old medical doctor and he likes Cuban food. Alice, Bob's wife, is 40 and an architect. She is very passionate about fashion design and shopping. Their son Charlie, sitting in the back of the car, is a technology-enthusiast teenager who is listening to his favorite indie rock music on his smartphone. Suppose there exists a mechanism for *profiling* passengers traveling in the same smart vehicle, either explicitly or implicitly. In other words, we assume the smart car can keep track of each passenger's profile. Such a profile needs to be built only from data the user agrees to share with the surrounding IoT environment.

Suppose these travelers are about to enter a city where an iconic summer music festival takes place. Interestingly, an emerging rock band is going to perform on stage that same evening. Festival promoters have already advertised that event through *analog* (e.g., newspapers and small billboards) and *digital* (e.g., the city's website) channels. However, they would also like to take advantage of an *IoT ad network* to send more targeted and dynamic sponsored messages, namely to reach out to possibly interested people who happen to be around, such as Charlie.

Assume Charlie receives an advertisement on the music app installed on his smartphone, and he convinces his parents to stop to attend the concert. Other similar advertising messages might be delivered to Alice and Bob as well. For example, Alice could receive a suggestion to visit the city's shopping mall on her dedicated portion of the car's head-up display. Furthermore, the eye-tracking sensors installed in the car could detect that Bob is getting tired, as he has been driving for too long. Therefore, Bob might be prompted with the coordinates of the best local Cuban cafe on the GPS along with a voice message suggesting to have a coffee there.

We propose an IoT advertising platform that behaves as an intermediary (i.e., a *broker*) between *advertisers* (the festival promoters), *end-users* (Alice, Bob, and Charlie), and possibly *publishers*, the same way well known ad networks operate in the context of Internet advertising. Note though that in IoT, several entities can play the role of "publisher," which is not limited to a single web resource provider, but may be a composite entity with several IoT devices. As such, the automaker, as well as any other device embedded in the car or dynamically linked to it, may act as a publisher. Assuming the IoT ad network can gather information from smart vehicles and passengers traveling in a specific geographic area, that information can be further matched against a set of candidate advertisements, which in turn are conveyed to the right target. Note that triggering ad requests is somewhat transparent to the end user, that is, we do not conjure any explicit publisher-subscriber mechanism between end users and advertisers. On the other hand, users must have control over their data, which in turn may be used by the IoT ad network for targeting.

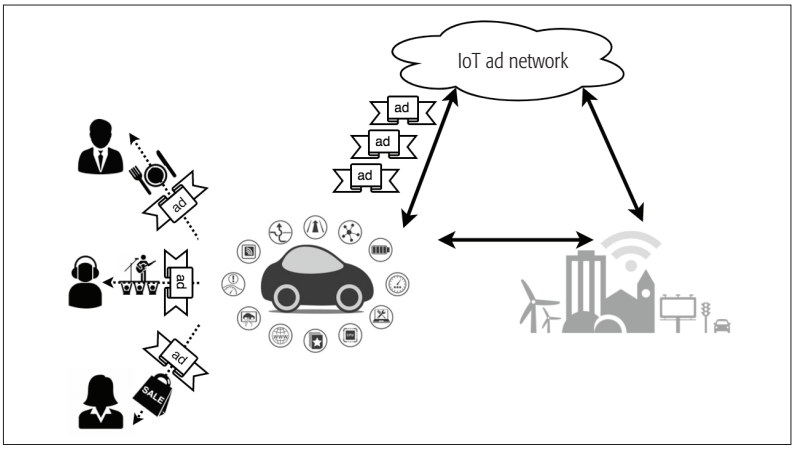

Figure 1. Targeted ads triggered by the IoT environment (e.g., a smart car traveling close by a smart city) are delivered to end users on IoT devices via an intermediate IoT ad network.

Figure 1 depicts the scenario above, where Alice, Bob, and Charlie all receive their targeted advertising messages. The IoT ad network is responsible for choosing the most relevant advertisements and delivers them through one or more IoT devices that are either embedded in the car (e.g., the head-up display and the GPS) or temporarily joined to the car (e.g., the passengers' smartphones).

We claim that IoT represents a huge opportunity for marketers who may want to leverage the IoT ecosystem to increase their targeted audience. Indeed, although online advertising is already a multibillion-dollar market, we believe one of its limitations is that it is essentially based on the activities users perform on the web. Instead, IoT advertising will overcome this limitation by bringing advertising messages to users interacting with the IoT environment (which is potentially much larger than the web).

How Internet Advertising Works Today

The general idea behind Internet advertising is to allow web content *publishers* to monetize by reserving some predefined slots on their web pages to display ads. On the other hand, *advertisers* compete for taking those slots and are keen on paying publishers in exchange for that. Actually, publishers often rely on third-party entities, called *ad networks*, that free them from running their own ad servers; ad networks decide on behalf of publishers which ads should be placed in which slots, when, and to whom. Furthermore, advertisers partner with several ad networks to optimize their return on investment for their ad campaigns. Finally, ad networks charge advertisers for serving their ads according to a specific *ad pricing model*, for example, *cost per mille impres-*

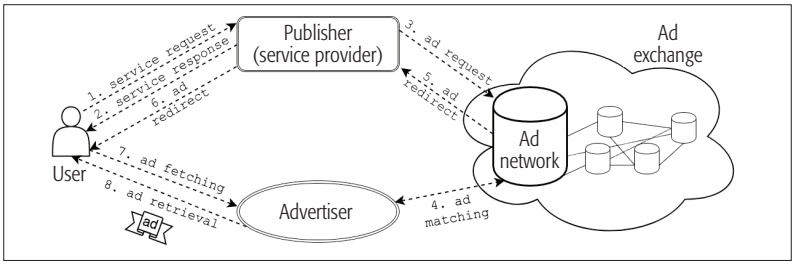

Figure 2. High-level architecture of traditional online advertising.

sions (CPM) or *cost per click* (CPC), and share a percentage of this revenue with the publishers where those ads are impressed [8].

At the heart of online advertising, there is a real-time auction process. This runs within an *ad exchange* to populate an ad slot with an *ad creative*.[1] For each ad request, there are multiple competing advertisers bidding for that ad slot. Before any ad is served, publishers and advertisers outline a number of ad serving requirements, such as budget, when the ad should be displayed, and targeting information. In particular, with *targeted advertising*, sponsored content can be delivered that is more likely tailored to each user's *profile*, which is either explicitly collected (e.g., through the set of user queries submitted to the search engine in the case of sponsored search) or implicitly derived (e.g., from user's browsing history in the case of native advertising) [10, 11]. The auction process uses all those requirements to match each ad request with the "best" ad creative so as to maximize profit for the publisher.

Figure 2 shows the high-level architecture of current online advertising systems. Although the actual architecture can be more complex than the figure, the main entities involved are: the *user* who typically sits behind a web browser or a mobile app; the *publisher* (i.e., a service provider) who exposes some "service" to the user (e.g., a web content provider like cnn.com or a web search engine like Google or Yahoo); the *advertiser* who wants to promote its products and possibly attract new customers by leveraging the user base of the publisher; and the *ad network* that participates in the *ad exchange* and acts as intermediary between the publisher and the advertiser.

The workflow is as follows:

- The user accesses a service exposed by the publisher, for example, using `HTTP GET` (1).
- The publisher responds with the "core" content/service originally requested (2).
- The publisher also asks its partner ad network to fetch ads that best match the user's profile, and are eventually shown to the user within the same content delivered before (3).
- The ad network uses profile information during the real-time auction, which takes place on the ad exchange to select advertisements that are expected to generate the highest revenue (4).
- The ad network instructs the publisher on how to tell the user how to fetch the selected ad (5–6).
- Finally, the user requests (7) and retrieves (8) the actual ad to be displayed.

As it turns out from the description above, there is a clear event that activates an ad request, that is, the user accessing a resource offered by a web publisher. Conversely, in the IoT world that triggering event might be less explicit (i.e., the user *interacting* with IoT devices). Nevertheless, we discuss how the scheme described above can be adapted to the context of future IoT advertising.

[1] An ad creative is the actual advertisement message (e.g., text and image) impressed on the slot.

IoT Key Features

The IoT stack is normally described as a four-layer infrastructure. The first layer defines how the smart physical world (e.g., networked-enabled devices, devices embedded with sensors) interact with the physical world. The second layer is in charge of providing the necessary connectivity between devices and the Internet. Further, a third layer incorporates data aggregation and other preliminary data processing. Finally, the fourth layer is in charge of feeding the control centers and providing IoT cloud-based services [12]. In general, IoT bounds a cooperative relationship among computing systems, devices, and users with these layers.

Connectivity: A crucial element in IoT is the high connectivity required among devices, servers, and/or service control centers. Indeed, high-speed connectivity is necessary in order to cope with real-time applications and the level of cooperation expected from IoT devices. Currently, IoT connectivity is guaranteed by traditional network protocols and technologies like WiFi, Bluetooth Smart, and Device-to-Device (D2D) communications. IEEE and the IETF are designing new communications protocols specifically devised for IoT [13]. These protocols (i.e., IEEE 802.15.4e, 6LoWPAN, LoRa) are intended to homogenize the IoT low-energy communication environment among the huge IoT device diversity.

Resource Availability: This defines the amount of computing resources available to implement IoT services. In general, IoT devices can be categorized into two groups: resource-rich, with faster CPUs and higher memory availability, and resource-limited devices, with limited memory and low-performance CPUs. Note that the way IoT devices interact with users (e.g., display availability, user-input enabled devices, and so on) depends on the available resources [14].

Power Consumption: The nature of IoT applications imposes several power constraints on the devices. In general, IoT devices are meant to be remotely monitored, autonomous, wearable, and/or with high mobility. These characteristics define the specific power restrictions for every application.

Complexity and Scalability: Today, IoT devices can be found in several user-oriented (e.g., smart home, wearable devices) and industrial (e.g., smart grid, healthcare IoT) applications. The different IoT architectures need to be scalable to handle the constant flow of new devices and the always-increasing set of new services and applications.

A Vision for an IoT Advertising Landscape

The ultimate aim of IoT is to provide new applications and services by taking advantage of the IoT features discussed above. Different from the simplistic approach of utilizing traditional legacy

sensors combined with decision entities, the high connectivity and intelligence present in IoT along with the possibility of continuous scalability, allow building a wide pool of applications based on user generated IoT data. Among those, expanding the traditional Internet advertising marketplace is one of the most promising.

To enable the IoT advertisement vision, we introduce our model of an IoT advertising architecture (Fig. 3). Although this is clearly inspired by the Internet advertising architecture (Fig. 2), IoT advertising has its own peculiarities, and therefore, deserves a dedicated infrastructure to be successful.

Our IoT advertising model consists of three layers, each one composed of several entities: the bottom layer (*IoT physical layer*) contains physical IoT devices; the middle layer (*IoT advertising middleware*) coincides with the *IoT advertising coordinator*, which allows physical IoT devices to interface with the upper layer (IoT advertising ecosystem), and in particular with the IoT publisher.

In the rest of this section, we discuss the role and characteristics of each entity separately.

IoT Advertiser

This represents an entity that would like to take advantage of IoT to advertise its own products/services, such as the music festival promoters in the use case discussed above. It is expected to interact with other actors in the advertising ecosystem in the same way web advertisers do with traditional Internet advertising. Due to the high diversity of devices involved, the IoT advertiser needs to conceive and design its campaign for heterogeneous targets, that is, newer ad formats that are not necessarily visual (e.g., acoustic messages), as opposed to traditional banners displayed on web browsers or mobile apps. Moreover, targeting criteria may go beyond just the user's demographics and/or geolocation; in fact, the contextual environment will play a crucial role in the ad-matching phase.

IoT Ad Network and IoT Ad Exchange

The IoT ad network, in combination with the IoT ad exchange, will be responsible for matching the most profitable ads with target IoT publishers on behalf of both the publisher and the advertiser. This can be achieved in the same way traditional ad networks interact with ad exchanges for Internet advertising, that is, through real-time auctions. Moreover, differently from Internet advertising where those auctions are triggered by the user requesting a resource from a web publisher, in IoT such events can be extremely blurry as the user keeps constantly interacting with their surrounding IoT environment. That means IoT ad networks and ad exchanges may need to operate at an even larger scale and higher rate.

IoT Publisher

The role of the IoT publisher is no longer limited to a web resource provider. Rather, an IoT publisher can be thought of as an ensemble of IoT devices, which collectively cooperate to implement and expose to the user multiple functionalities, as well as to deliver advertisements. For instance, the smart vehicle introduced in our use case is a possible example of an IoT publisher. The smart vehicle is indeed composed of several embedded IoT atomic devices (e.g., the GPS, the tire controller, the sound system), each one implementing its own communication standard and exposing a specific functionality through its own user interface. In addition, many other IoT devices can dynamically and temporarily join the smart vehicle (e.g., the smartphones of car passengers).

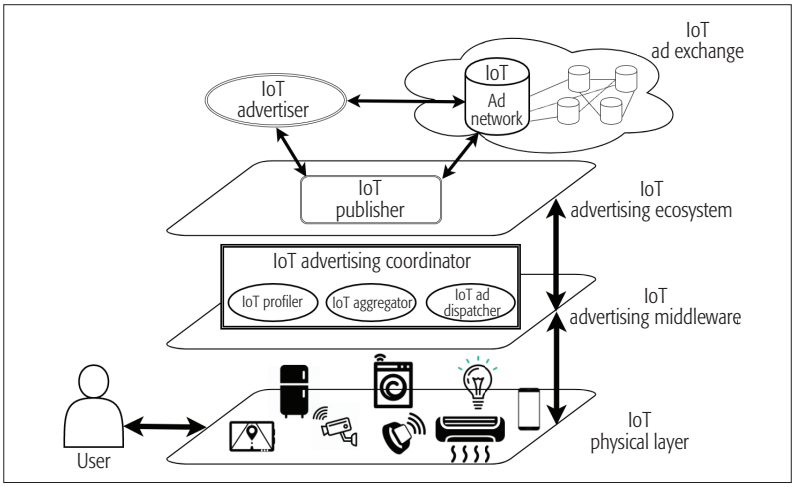

Figure 3. The proposed IoT advertising model consists of three layers: IoT Physical Layer, IoT Advertising Middleware, and IoT Advertising Ecosystem.

IoT Advertising Coordinator

The role of the IoT advertising coordinator is twofold. On the one hand, it allows bottom-layer IoT devices to expose themselves as a single IoT publisher entity to the upper-layer advertising ecosystem. On the other hand, it is responsible for dispatching and delivering advertisements coming from the advertising ecosystem down to physical IoT devices, and in turn, to the end user. To achieve both of those capabilities, the IoT advertising coordinator makes use of several subcomponents. Among those, we focus on three: *IoT aggregator*, *IoT profiler*, and *IoT ad dispatcher*. These subcomponents are responsible for:

- Unifying different communication standards utilized in a vast variety of IoT devices, so they can all respond to the specific advertisement needs.
- Providing a cross-platform that will translate IoT-customer interaction into usable data for real-time effective advertisement (i.e., collecting meaningful metadata or "*profiles*," which can, in turn, be exploited during ad matching at the layer above).
- Managing the actual delivery of advertisements to the target IoT device, and therefore to the user, according to specific supported ad formats.

More specifically, the ability of the IoT advertising coordinator to take advantage of IoT devices and user identification via digital fingerprinting will open the door to new advertising strategies. These might consider the following key aspects.

User Profile: IoT advertising will vary based on the actual recipient (age range, gender, known user behavior) so we can have ads anticipating the

IoT device heterogeneity will add an extra burden to the IoT advertising coordinator. The coordinator would need to deal with different memory, CPU, energy, and sensor availability and capabilities, so the right advertising strategy is chosen for every device and user while keeping the required efficiency and reliability of services.

user's needs not based on what they browse, but rather based on what they are and what they do.

Context Awareness: IoT advertising will adapt to new contexts, that is, the advertisement strategy will also focus on the location, time, and the type of activity the user is performing (e.g., a regular traveler can receive ads based on the most visited restaurants and hotels during lunchtime).

Services/Features: The IoT advertising ecosystem can make use of an unlimited number of features to know more about the user (e.g., most visited locations, driving mode, behavioral characteristics). That will translate into a new set of services from the IoT advertising landscape (e.g., announcing upcoming events with better price deals, lower car insurance due to the driver record directly derived from the smart car, and so on).

Security/Privacy: User security and privacy protection will impact the new IoT advertising model in two different ways. First, the coordinator needs to be transparent to the implementation of traditional (or any new) IoT security mechanisms. Second, these security mechanisms will inevitably limit the amount and type of data that can be extracted from IoT devices and will affect the quality of the user's digital fingerprint.

Device Capabilities: The coordinator may have to deal with devices supporting a broader spectrum of advertising formats by themselves (e.g., smartwatches have full display capabilities and adequate computing resources). Conversely, other devices would either accept only custom, resource-friendly ad formats (e.g., acoustic messages sent to smart speakers) or rely on other devices with more capabilities (e.g., the smart lighting system may use the client application running on the smartphone to interact with the user). In this regard, the ad dispatcher will have a crucial role in deciding which specific types of ads to generate/integrate from/to the different devices and how those ads can be delivered to the user.

Furthermore, the sensors present in smart devices and interacting with users will play a major role in profiling what the user does (e.g., the presence sensor can report when the user leaves the house) and the specific context of such activities (e.g., Saturday night). These constitute key elements for more effective advertising (e.g., restaurants and nightclubs). Eventually, to be fully effective in a fast-changing and very limited power-consuming IoT world, the amount of data required to characterize users needs to be minimized while coping with the demand imposed by the proposed IoT advertising model. In this context, the IoT advertising coordinator will "translate" data flow from/to IoT devices into a common language and, more importantly, it will adapt IoT requirements to the well known Internet advertising model to enable the new IoT advertising ecosystem. Finally, timing and geographical distribution of sensors will influence the effectiveness of the IoT advertising coordinator by (1) effectively using user location and IoT device availability to deliver the most appropriate ad (e.g., take advantage of the presence of electronic road signals to show ads to drivers) and (2) deliver in a timely manner the right apps (e.g., nearby preferred restaurants at lunchtime).

Challenges of IoT Advertising

In this section, we analyze the possible key challenges of IoT advertising.

Architectural Challenges

From the IoT advertising perspective, the current IoT architecture has several challenges that need to be addressed. IoT device heterogeneity will add an extra burden to the IoT advertising coordinator. The coordinator would need to deal with different memory, CPU, energy, and sensor availability and capabilities, so the right advertising strategy is chosen for every device and user while keeping the required efficiency and reliability of services. Moreover, IoT can be configured in several different network topologies, which require the use of different network metrics to characterize the IoT traffic and to successfully identify devices and users.

Ad Content Delivery Challenges

Content delivery in IoT advertising involves three different scopes: user profile, user location-activity, and device capabilities. Content delivery challenges will defy the capacity of the IoT devices to cope with the requirements of the proposed IoT advertising scheme in two main aspects.

Quality and Quantity of Available User Data: Different levels of data obtained from the user will create user-based digital signatures (i.e., user profiles) with different quality levels. Also, different permission policies can impact negatively on the quality of users' activity/location tracking processes.

Device Capabilities: In cases where IoT device cooperation is not possible, the delivery of the advertisement content to the user will be exclusively defined by the device capacity. For instance, the amount of advertisement content that the user can get from devices with visual capabilities is expected to be higher.

Security and Privacy Challenges

Integrating IoT into the traditional advertising model poses security challenges for customers, advertisers, and publishers. Some of the security challenges that need to be overcome are the following:

- Due to the high diversity of devices and communication protocols in IoT, there exists a perpetual need for monitoring and detecting new vulnerabilities and attacks in a constantly changing environment.
- Sensitive user data needs to be protected not only from outsiders, but also from malicious corporations that can misuse it.
- Users are not always aware of security risks and much effort needs to be made on the educational side.
- Current and new communication protocols incorporate state-of-the-art protection mechanisms, but in most cases security is optional and these protocols are insecure in default mode.
- The high level of interconnection in the IoT creates more opportunities for malware and worms to spread over the network.

- Advertisements should not become intrusive on user privacy nor disrupt the user experience of the surrounding IoT environment.

Traditionally, Internet advertising has compromised user privacy by tracking people's browsing habits. IoT advertising would go further by tracking user behavior based on day-to-day activities. Here, *dataveillance* becomes more valuable considering that IoT user data is much more diverse if compared with regular web browsing data.

Fragmentation of IoT

Currently, there is not a single inter-operable framework that integrates all IoT devices and services. In fact, despite the efforts to design dedicated protocols for IoT [13], the current IoT ecosystem offers several options for developers to write smart apps using a variety of different programming architectures (e.g., SmartThings, OpenHAB, and Apple Home Kit). Also, multiple combinations of standards and protocols are possible (e.g., communications: IPv4/IPv6, RPL, 6Low-PAN; data: MOTT, CoAP, AMPQ, Websocket; device management: TR-069, OMA-DM; transport: Wifi, Bluetooth, LP-WAN, NFC; device discovery: Physical Web, mDNS, DNS-SD; device identification: EPC, uCode, URIs). The proposed IoT advertisement middleware should be able to adapt and convert the current fragmentation of the IoT world into a common language to enable IoT advertising.

IoT Data Flow

Data flow in IoT highly depends on the programming architecture. There are few cases where smart apps run on specific IoT devices or hubs; however, most of the IoT apps are cloud-based [15]. Smart apps obtain information from the smart devices (sensors) and send data to the cloud to execute the app logic. External web programming tools like IFTTT and Node-RED can also be integrated into the IoT architecture to connect, control, and request information from different devices. The integration of these third-party applications can also represent a challenge to the proposed IoT advertising model. On the other hand, such integration would simplify the overhead caused by the current IoT fragmentation.

Conclusions

The Internet advertising market is worth hundreds of billions of dollars and is one of the fastest growing online businesses. Nevertheless, it is still restricted to web browser-based and, more recently, mobile in-app contexts.

The Internet of Things (IoT) will open up a novel, large-scale, pervasive digital advertising landscape; in other words, a new IoT advertising marketplace that takes advantage of a huge collection of smart devices, such as wearables, home appliances, vehicles, and many other connected digital instruments, which end users constantly interact with in their daily lives.

In this article, we introduced the architecture of an IoT advertising platform and its enabling components. We also discussed possible key challenges to implement such a platform with a special focus on issues related to advertisement delivery, security, and privacy of the user.

To the best of our knowledge, this is the first work defining IoT advertising and discussing possible enabling solutions for it. We expect our work will impact both upcoming research on this topic, and the development of new products at scale in the industry.

Acknowledgment

This work is partially supported by the U.S. National Science Foundation (Awards: NSF-CA-REER-CNS-1453647, 1663051). Mauro Conti is supported by a Marie Curie Fellowship funded by the European Commission (agreement PCIG11-GA-2012-321980). This work is also partially supported by the EU TagItSmart! Project (agreement H2020-ICT30-2015-688061); the EU-India REACH Project (agreement ICI+/2014/342-896); the project CNR-MOST/ Taiwan 2016-17 "Verifiable Data Structure Streaming," grant no. 2017-166478 (3696) from the Cisco University Research Program Fund and Silicon Valley Community Foundation; and by the grant "Scalable IoT Management and Key security aspects in 5G systems" from Intel. The views in this document are those of the authors, not of the funding agencies.

Additional Note

The authors are listed in alphabetical order and each of them equally contributed to this work.

References

[1] "IAB Internet advertising revenue report 2012 full year results," http://www.iab.net/media/file/IAB Internet Advertising Revenue Report FY 2012 rev.pdf, Apr. 2013; accessed on: 21 Jan. 2018.

[2] "Worldwide Ad Spending: The eMarketer Forecast for 2017," https://www.emarketer.com/Report/ Worldwide-Ad-Spending-eMarketer-Forecast-2017/2002019?ecid=adx103, Apr. 2017; accessed on: 21 Jan. 2018.

[3] "Worldwide Ad Spending: eMarketer's Updated Estimates and Forecast for 20152020," https://www.emarketer.com/Report/ Worldwide-Ad-Spending-eMarketers-Updated-Estimates-Forecast-20152020/ 2001916, Oct. 2016; accessed on: 21 Jan. 2018.

[4] B. J. Jansen and T. Mullen, "Sponsored Search: An Overview of the Concept, History, and Technology," *IJEB*, vol. 6, no. 2, 2008, pp. 114–31.

[5] H. Becker *et al.*, "Context Transfer in Search Advertising," *Proc. SIGIR '09*, ACM, 2009, pp. 656–57.

[6] J. Azimi *et al.*, "Visual Appearance of Display Ads and its Effect on Click Through Rate," *Proc. CIKM '12*, ACM, 2012, pp. 495–504.

[7] J. Qin *et al.*, "POST: Exploiting Dynamic Sociality for Mobile Advertising in Vehicular Networks," *IEEE Trans. Parallel Distributed Systems*, vol. 27, no. 6, June 2016, pp. 1770–82.

[8] G. Chen *et al.*, "In-Depth Survey of Digital Advertising Technologies," *IEEE Commun. Surveys Tutorials*, vol. 18, no. 3, 3rd Quarter 2016, pp. 2124–48.

[9] M. Lalmas *et al.*, "Promoting Positive Post-Click Experience for In-Stream Yahoo Gemini Users," *Proc. KDD '15*, New York, NY, USA: ACM, 2015, pp. 1929–38.

[10] J. Yan *et al.*, "How Much Can Behavioral Targeting Help Online Advertising?" *Proc. WWW '09*, New York, NY, USA: ACM, 2009, pp. 261–70.

[11] K. Li and T. C. Du, "Building a Targeted Mobile Advertising System for Location-Based Services," *Decision Support Systems*, 2012, pp. 1–8.

[12] S. A. Al-Qaseemi *et al.*, "Iot Architecture Challenges and Issues: Lack of Standardization," *Proc. 2016 Future Technologies Conference (FTC)*, Dec. 2016, pp. 731–38.

[13] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues," *IEEE Commun. Surveys Tutorials*, vol. 17, no. 3, 3rd Quarter 2015, pp. 1294–1312.

[14] L. Babun, H. Aksu, and A. S. Uluagac, "Identifying Counterfeit Smart Grid Devices: A Lightweight System Level Framework," *Proc. 2017 IEEE Int'l Conf. Commun. (ICC)*, May 2017, pp. 1–6.

The Internet of Things will open up a novel, large-scale, pervasive digital advertising landscape; in other words, a new IoT advertising marketplace that takes advantage of a huge collection of smart devices, such as wearables, home appliances, vehicles, and many other connected digital instruments, which end users constantly interact with in their daily lives.

[15] E. Fernandes, J. Jung, and A. Prakash, "Security Analysis of Emerging Smart Home Applications," *Proc. 2016 IEEE Sym posium on Security and Privacy (SP)*, May 2016, pp. 636–54.

Biographies

Hidayet Aksu received his Ph.D. degree from the Department of Computer Engineering, Bilkent University. He is currently a postdoctoral associate in the ECE Department at Florida International University. Before that, he conducted research as a visiting scholar at IBM T.J.Watson Research Center, USA, for one year. His research interests include security for cyber-physical systems, Internet of Things, IoT security, security analytics, social networks, big data analytics, distributed computing, wireless ad hoc and sensor networks, and p2p networks.

Leonardo Babun is currently a Ph.D. student and research assistant in the Department of Electrical and Computer Engineering at Florida International University, as a member of the Cyber-Physical Systems Security Lab (CSL). He previously completed his M.S. in electrical engineering in the Department of Electrical and Computer Engineering at Florida International University in 2015. His research interests are focused on cyber physical systems (CPS) and Internet of Things (IoT) security and privacy.

Mauro Conti is an associate professor at the University of Padua, Italy. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a post-doc researcher at VU Amsterdam, The Netherlands. He has been a visiting researcher at GMU, UCLA, UCI, FIU, and TU Darmstadt. He has been awarded with a European Marie Curie Fellowship, and with a German DAAD Fellowship. He is senior member of the IEEE.

Gabriele Tolomei is an assistant professor at the University of Padua, Italy. Previously, he was a research scientist at Yahoo Research in London, UK. He received his Ph.D. in computer science from Ca' Foscari University of Venice, Italy in 2011. His research interests are: web search, machine learning, and computational advertising. He has authored approximately 30 papers in prestigious international journals and conferences, and four U.S. patents. He is PC member of many IEEE and ACM conferences.

Selcuk Uluagac leads the Cyber-Physical Systems Security Lab at Florida International University, focusing on security and privacy of Internet of Things and cyber-physical systems. He has a Ph.D. and M.S. from Georgia Institute of Technology, and an M.S. from Carnegie Mellon University. In 2015, he received the U.S. National Science Foundation CAREER award and the U.S. Air Force Office of Sponsored Research Summer Faculty Fellowship, and in 2016, the Summer Faculty Fellowship from University of Padova, Italy.