Dashbell: A Low-cost Smart Doorbell System for Home Use

Bradley Quadros, Ronit Kadam
Devendra Lavaniya, and Muhammad Mukhtar
Department of EECS, University of California, Irvine
Irvine, CA92617, USA
Email: {bquadros, kadamr, dlavaniy, mohamme}@uci.edu

Kartik Saxena, Wen Shen and Alfred Kobsa
Department of Informatics
University of California, Irvine
Irvine, CA92617, USA
{saxenak, wen.shen, kobsa}@uci.edu

Abstract—Smart doorbells allow home owners to receive alerts when a visitor is at the door, see who the guest is, and communicate with the visitor from a smart device. They greatly improve people's life quality and contribute to the evolution of smart homes. However, the commercial smart doorbells are quite expensive, usually cost more than 190 US dollars, which is a substantial impediment on the pervasiveness of smart doorbells. To solve this problem, we introduce the Dashbell-a budget smart doorbell system for home use. It connects a WiFi-enabled device, the Amazon Dash Button, to a network and enables the home owner to answer the bell triggered by the dash button using a smartphone. The Dashbell system also enables fast fault detection and diagnosis due to its distributed framework.

I. INTRODUCTION

Doorbells have been playing an important role in protecting the security of modern homes since they were invented [1] [2]. A doorbell allows visitors to announce their presence and request entry into a building as well as enables the occupant to verity the identity of the guests to help prevent home robbery or invasion at a moment's notice [1]. There are two types of doorbells depending on the requirement of wall wiring: the wired doorbells and the wireless doorbells [3] [2]. The former requires a wire to connect both the front door button and the back door button to a transformer, while the latter transfer the signal wirelessly using telephone technology [3] [2].

Modern buildings are typically equipped with wireless doorbell systems that employ radio technology to signal doorbells and answer the doors remotely. Although these doorbells are much more convenient than wired ones, they do not always satisfy the demands of modern homes for the following three reasons. First, the answering machines are normally located at a fixed place (often near to the door), if a occupant wants to answer the doorbell, he/she has to go to the answering machines. Second, if the occupant would like to see the visitors outside, he/she has to go to door. Third, the occupant has no way to answer or admit guests when he/she is not at home, nor to keep a record of guests.

As smart home technology matures, smart doorbells can solve this problem greatly by connecting the doorbells to the Internet(or a local network) and allowing users to answer the bell through a smart device such as a smartphone or tablet [4] [5] [6] [7]. This enables a home owner to answer and admit a visitor anywhere when a smart device connecting to the Internet is available [8] [9]. However, such smart doorbells are quite expensive (usually more than 190 US dollars) due to technical and manufacturing difficulties [10] [11] [12]. The high prices make these products unavailable to most home users with limited budgets, hindering the pervasiveness of smart doorbells. This is confirmed by a research shows that less than 4% of U.S. households have a smart doorbell system to protect the security of the homes [13]. To solve this problem, we introduce the Dashbell- a low-cost smart doorbell system for home use. The doorbell system uses a cheap, WiFi-enabled device-the Amazon Dash Button to serve as the doorbell, and connects it to the Internet, allowing users to answer the bell anywhere using a smart device such as a smartphone or a tablet. With such as solution, users may purchase a smart doorbell system at a price as low as 40 US dollars, which significantly increases the affordability of the smart doorbells.

II. RELATED WORK

A. Smart Doorbells

A smart doorbell is an integral part of a smart home, which helps protect the security of the home by avoiding unwanted access such as robbery and invasion [4] [5] [6] [7]. The controller of the smart home can potentially answer the bell and decide whether to admit a visitor outside the door or not through adaptive learning and other technologies [14]. Because of the important role that smart doorbells play on building a smart home, many techniques and methodologies have been invented during past few years [7] [15] [16] [17].

The existing smart doorbells provide an integrated solution, which means that the working mechanisms or the implementation details are hidden and unknown to the users. If there is a failure, users have to seek help from professionals for repairs or maintenance. It is also very likely that users need to replace the whole smart doorbells due to a failure of a component in the system.

B. Dash Button

Amazon Dash Button is a WiFi-enabled device that allows consumers to reorder frequently used daily products like trash bags, toilet towels or refill blades [18] [19] [20] [21] by pressing a button. A dash button can be purchased via online

and costs 4.99 US dollars [18]. Recently, it has been found that the dash button can be tweaked to track baby habits [22]. We employ this feature of the dash button and use it as a doorbell (or a trigger) of the Dashbell system.

Alternatives to Dash Button include portable door bell kits, and wireless door chime trigger with motion sensors, both of which can be purchased for less than 5 US dollars.

III. DASHBELL: A LOW-COST SOLUTION

The Dashbell enables the home owner to see the pictures of a visitor to remotely ascertain their identity. Besides, it allows the home owner to admit or reject a request anywhere when connected to the Internet. The Dashbell system (as shown in Fig. 1) consists of a dash button(as the doorbell), a WiFi router, a computing device(e.g., a Raspberry Pi), a webcam, a buzzer, cloud computing service (e.g., Amazon Web Service), a smartphone and the Internet. The working flow is described as follows:

1) A visitor presses the dash button to request for entry to the home.
2) A signal from the Dash button to the WiFi router is captured by the Raspberry Pi. It triggers the following operations: activate the webcam and take a picture of the guest who pressed the button; activate the buzzer for the alarm sound so that the owner is notified on the presence if inside the house; the image captured along with the timestamp is uploaded to the cloud.
3) The webcam takes pictures of the guest and process and sends them to the cloud database service (We use Amazon Web services).
4) The service notifies the user through the mobile app (We develop an Android app).
5) The home owner decides whether to grant access to the visitor. The decision is updated on the server, which also delivers this message to the Raspberry Pi. If the home owner grants the access to the visitor, the door automatically opens using a servo-motor. If the access is denied, no actions will be taken and the guest's request for entry is denied.

The home owner has a variety of options to choose regarding this call: accept the call or reject the call if the service is on, or ignore the call if the "Do Not Disturb" is on. If the user grants the access of the guest, the message will be delivered to the Raspberry Pi by updating the database. The owner is able to view the historical record of the requests. The user interface also enables the user to choose three types of alerts: Email, Text Message, and Ringer. The user interface of the mobile application is shown in Fig. 2.

We are using Amazon Web Service (AWS) cloud services for this implementation. We have a EC2 linux instance running which hosts a MySQL DB server as well as an Apache Web Server. The server maintains a TCP connection with the Raspberry Pi by listening on a specific port. When it receives the data object with the timestamp and the picture, it will be uploaded to the web server and a link is shared with the DB server, which maintains a database for all the entries.

Additionally it maintains a column for "Access Granted" as a binary"Yes" and "No" value, initialized as "Null" and updated with the user's response . Another TCP connection is maintained by the server with the user's mobile client on a separate port. It pushes when new data is received to the user's mobile device as a notification triggered by the mobile application. When the user clicks on the notification, it shows the picture of the user and allows user to either grant or deny access as per his/her discretion. Other features offered by the mobile applications are explained below. The response is relayed back to the server and "Access Granted" field is updates as "Yes" or "No" based on the response. This triggers another action in DB server and the response data is sent back to the Raspberry Pi.

IV. DISCUSSION

Modern homes are typically equipped with Wi-Fi routers and have access to the Internet. Smartphones are also highly available to the majority of population. To build a budget smart doorbell system like Dashbell, the user only needs to purchase a Amazon Dash Button (5 dollars), a Raspberry Pi (25 dollars), a webcam (8 dollars), and a buzzer(1 dollar). The user can sign up to request for free Amazon Web Service. The total cost of a Dashbell system is less than 40 US dollars.

The Dashbell system differentiates existing smart doorbell systems in the following aspects. First, Dashbell is much cheaper than existing smart doorbells. Second, Dashbell is a distributed system rather than an integrated one, which enables faster fault detection and diagnosis. For instance, if some of the components fail to operate, one can just identify and fix or replace the parts by checking each individual device instead of disassembling or replacing the whole doorbell system. Third, given that most smart doorbell devices are expensive devices, they can be potentially detached and stolen. However, with the Dashbell, only the Dash button, which is inexpensive and replaceable, needs to be placed outside the home, making it a much better alternative in terms of the device's own security. Lastly, unlike exisiting smart doorbells, which are only sold in limited places and through particular channels, the components of the Dashbell system are highly available.

While the Dashbell provides several useful features and enhanced security over a conventional doorbell, there are a few security and privacy issues associated with it. Since the device is connected via a home WiFi network, it is possible to compromise the network and use the device, grant access to unauthorized visitors or collect data using it without the owners consent. We advise users to keep their network secured with a password. Our system also takes pictures of visitors without their consent and stores them on the server. Since this is personally identifiable information, we have made sure the server and all communication channels are secure. Using secure communication channels and encrypting user data while storing on the server would be helpful in this regard. The mobile application also has an additional layer of security so that only owner can grant access to a visitor.
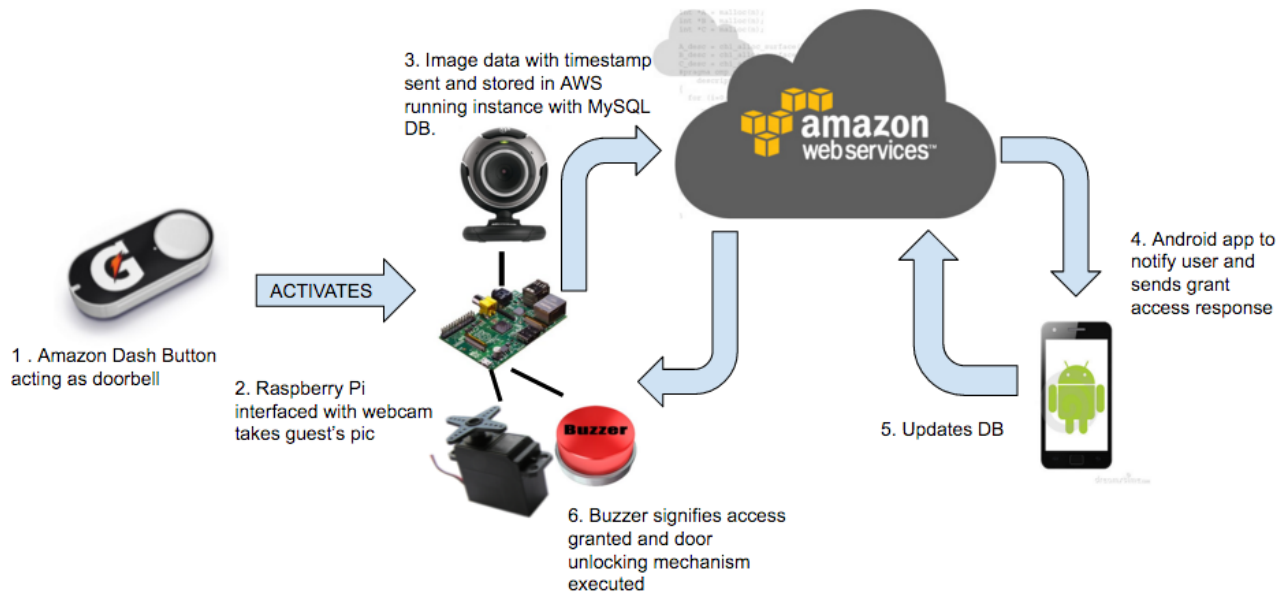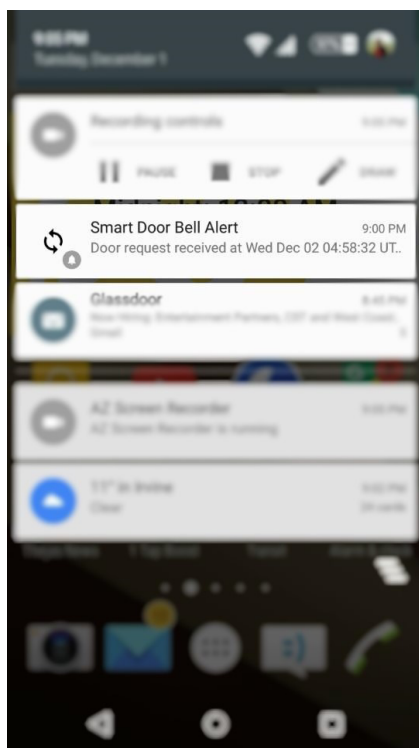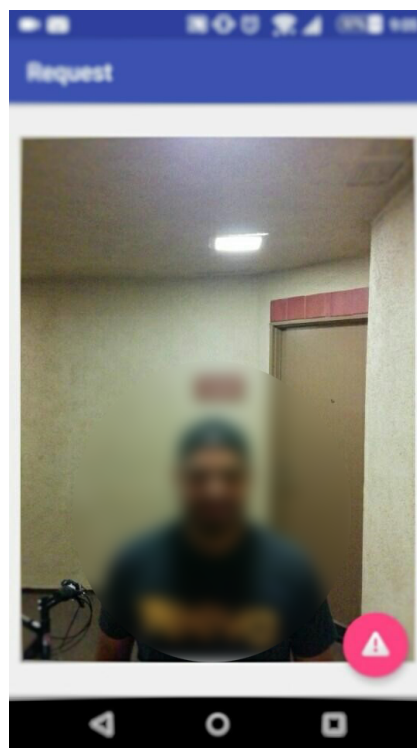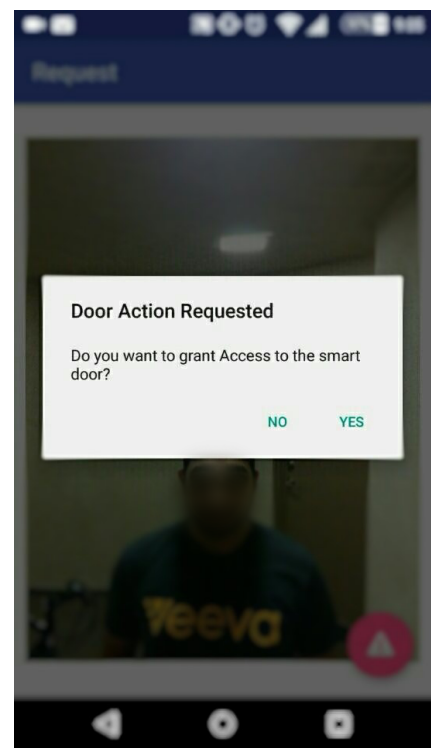
Fig. 1: The architecture of DashBell.

(a) Notification

(b) Visitor Picture

(c) Grant Access

Fig. 2: The user interface of the mobile application: (a) shows the notification on the phone received from the server.(b) Shows the picture of the visitor on the mobile application. The owner can click on the alert icon in the bottom right corner to show the access prompt. (c) shows the screen where the use can choose to accept or decline the visitor which will subsequently the door based on their decision. We will also have the option to scroll across a timeline and expand on the request made on a particular day. On clicking a particular request the owner will be directed to the next screen at where he / she will have a more detailed result of the request made at the selected time. The owner will also be provided with the settings page as shown in where configurable options for service enabling and notifications will be mentioned.

V. FUTURE WORK

In future work, we plan to implement one-way or two-way audio and video communication between the visitor and the homeowner. Further, we will integrate face recognition, natural language processing and machine learning techniques (e.g., Support Vector Machines, Neural Networks) to allow the Dashbell system to answer the door automatically without human intervention.

We found that the internals of the button are much more interesting and powerful than advertised [23] as it contains a proprietary chip inside which contains a small ARM processor, flash memory and a microphone besides the WiFi module. However, due to inaccessible SDK and no APIs, it is nontrivial to use them. Nevertheless, if similar programmable devices with open APIs can be used, it is possible to create even lower cost doorbells with the button as a standalone device and microphone to record guests' voice and identity to make decisions.

We also propose to conduct a user study to evaluate the reliability and the usability of the Dashbell system upon finishing the development. This will also help us understand if users have any privacy concerns regarding the use of this device.

VI. CONCLUSION

To increase the availability of smart doorbells, we introduce the Dashbell-a smart doorbell system that utilizes the Amazon dash button and existing devices in modern homes to develop a budget solution for users. The Dashbell system has the similar functionality with its commercialized counterparts with a much lower price. It costs less than 40 US dollars compared to 199 US dollars for a single smart doorbell available in market. The Dashbell employs a distributed approach, which enables fast fault detection and diagnosis. By doing so, we spread the benefits that smart doorbells bring to home users and contribute to building a smarter and better world through technology.

REFERENCES

[1] R. J. Robles, T.-h. Kim, D. Cook, and S. Das, "A review on security in smart home development," *International Journal of Advanced Science and Technology*, vol. 15, 2010.

[2] A. H. MOHAMMAD, "Of electronic door bell with counter and display," Ph.D. dissertation, 2009.

[3] H. V. Shah, G. Y. Tsao, A. L. Arizpe, and A. S. Oztaskin, "Doorbell mechanism using protection domains," Dec. 14 2010, uS Patent 7,853,957.

[4] M. Senagala, "Rethinking smart architecture: Some strategic design frameworks," *International Journal of Architectural Computing*, vol. 4, no. 3, pp. 33–46, 2006.

[5] J. C. Augusto and C. D. Nugent, "Smart homes can be smarter," in *Designing Smart Homes*. Springer, 2006, pp. 1–15.

[6] D. Cook and S. Das, *Smart environments: technology, protocols and applications*. John Wiley & Sons, 2004, vol. 43.

[7] S. Vig and S. Vig, "Smart doorbell security system and method to identify visitors," Aug. 23 2010, uS Patent App. 12/861,427.

[8] G. Demiris, B. K. Hensel *et al.*, "Technologies for an aging society: a systematic review of smart home applications," *Yearb Med Inform*, vol. 3, pp. 33–40, 2008.

[9] D.-M. Han and J.-H. Lim, "Design and implementation of smart home energy management systems based on zigbee," *Consumer Electronics, IEEE Transactions on*, vol. 56, no. 3, pp. 1417–1425, 2010.

[10] S. Higginbotham, "Connected doorbells might become the new hot smart home accessory," May 21 2015.

[11] D. Leclair, "What is a smart doorbell, and which should you buy?" 27 2014.

[12] A. Baker, "See when opportunity knocks with these smart doorbells," 21 2015.

[13] M. Hinkle, "Evolution of smart home and the internet of things," Nov. 22 2014, parksassociates.com.

[14] O. Lehmann, M. Bauer, C. Becker, and D. Nicklas, "From home to world-supporting context-aware applications through world models," in *Pervasive Computing and Communications, 2004. PerCom 2004. Proceedings of the Second IEEE Annual Conference on*. IEEE, 2004, pp. 297–306.

[15] T. J. Huisking, "Method and apparatus for unlocking/locking a door and enabling two-way communications with a door security system via a smart phone," Sep. 7 2012, uS Patent App. 13/606,690.

[16] C.-t. Yang and S.-h. Liu, "Smart doorbell with energy saving method," May 21 2015, uS Patent 20,150,138,353.

[17] A. M. Fadell, M. L. Rogers, Y. Matsuoka, D. Sloo, S. Honjo, S. A. McGaraghan, M. Plitkins, M. Veron, and I. Guenette, "Visitor feedback to visitor interaction with a doorbell at a smart-home," Dec. 31 2014, uS Patent App. 14/587,966.

[18] Amazon, "Amazon dash button," Nov. 22 2015, amazon.com.

[19] P. Fernandez and M. Kesselman, "Thinking through the internet of things," *Library Hi Tech News*, vol. 32, no. 5, 2015.

[20] S. ELLIS, "Honoring," *Chance*, vol. 88, p. 65.

[21] I. Crouch, "The horror of amazon's new dash button," 2 2015.

[22] T. Benson, "How i hacked amazon's 5-dollar wifi button to track baby data," Aug. 10 2015.

[23] R. Baguley, "Amazon dash: Hack it to run your own code," Aug. 12 2015, hackaday.com.