Sistemas & Telemática
ISSN: 1692-5238
EditorSyT@icesi.edu.co
Universidad ICESI
Colombia

Banerjee, Amit; Sameen Chishti, Mohd; Kumar, Sunjay
Implementing secure smart home using existing infrastructure
Sistemas & Telemática, vol. 15, núm. 43, 2017, pp. 9-18
Universidad ICESI
Cali, Colombia

Original research / Artículo original / Pesquisa original - Tipo 1

Implementing secure smart home using existing infrastructure

Amit Banerjee, Ph.D / amit@cs.sau.ac.in

Mohd Sameen Chishti, MCA / mohdsameen@gmail.com / http://orcid.org/0000-0003-3977-8488

Sunjay Kumar, MSc / sanjay09sw93@hotmai.com

Department of Computer Science, South Asian University, New Delhi, India

ABSTRACT The emergence of Internet of Things [IoT] paves the path of the smart home. A smart home learns the habits of residents to make intelligent decision, which requires knowledge to be communicated and stored. The communication of generated data creates loop-hole in security and privacy of the user of smart home. Another challenging issue while designing a smart home is that legacy home appliances lack the smart connectivity. This paper focuses on designing a secure architecture to access smart home appliances, while using the existing home appliances that lacks networking and processing power like a bulb or fan. To ensure secure communication using internet, we are using third party authentication tool deployed in cloud. We have installed a gateway as the entry point to our smart home and connected all the appliances to it. The user is authenticated by authentication server and gets access to the services. For implementation purpose, we used Kerberos as authentication tool and DragonBoard as gateway.

KEYWORDS DragonBoard; Kerberos; security; smart home.

Implementación de casas inteligentes seguras usando infraestructura existente

RESUMEN La aparición de IoT abre el camino de la casa inteligente. Una casa inteligente aprende los hábitos de los residentes para tomar decisiones inteligentes, lo que requiere conocimientos para ser comunicados y almacenados. La comunicación de los datos generados crea bucle en la seguridad y la privacidad del usuario de la casa inteligente. Otro problema difícil al diseñar una casa inteligente es que los electrodomésticos heredados carecen de la conectividad inteligente. Este documento se centra en el diseño de una arquitectura segura para acceder a electrodomésticos inteligentes, mientras que el uso de los electrodomésticos existentes que carece de red y procesamiento de energía como un bulbo o un ventilador. Para garantizar una comunicación segura mediante Internet, estamos utilizando una herramienta de autenticación de terceros desplegada en la nube. Hemos instalado una puerta de enlace como el punto de entrada a nuestra casa inteligente y conectado todos los electrodomésticos a la misma. El usuario es autenticado por el servidor de autenticación y obtiene acceso a los servicios. Para propósitos de implementación, utilizamos Kerberos como herramienta de autenticación y DragonBoard como puerta de enlace.

PALABRAS CLAVE DragonBoard; Kerberos; seguridad; casa inteligente.

Implementação do Secure Smart Home usando infraestrutura existente

RESUMO O surgimento do IoT abre o caminho da casa inteligente. Uma casa inteligente assimila os hábitos dos moradores para tomar decisões inteligentes, o que exige que o conhecimento seja comunicado e armazenado. A comunicação de dados gerados cria uma lacuna na segurança e privacidade do usuário da casa inteligente. Outro problema desafiador ao projetar uma casa inteligente é que os antigos eletrodomésticos não possuem conectividade inteligente. Este artigo foca-se na concepção de uma arquitetura segura para acessar eletrodomésticos inteligentes, enquanto usa os aparelhos domésticos existentes que não possuem rede e energia de processamento como uma lâmpada ou ventilador. ara garantir uma comunicação segura usando a internet, estamos usando uma ferramenta de autenticação de terceiros implantada na nuvem. Temos instalado um gateway como ponto de entrada para nossa casa inteligente e conectamos todos os aparelhos a ele. O usuário é autenticado pelo servidor de autenticação e obtém acesso aos serviços. Para fins de implementação, usamos Kerberos como ferramenta de autenticação e DragonBoard como gateway.

PALAVRAS-CHAVE DragonBoard; Kerberos; segurança; casa Inteligente.

Received / Recepción: Octubre 6, 2017 - Accepted / Aceptación: Octubre 30, 2017 *doi:10.18046/syt.v15i43.2710*

I. Introduction

Smart home are increasingly becoming a trend in modern lifestyle. A comfortable home is source of happiness, health and good conscience in human life. The development of Information and Communication Technology [ICT] take homes to an entirely new level where a home can feel, learn and think itself. The home learns the habits of person living there and acts accordingly. Although this definition of a smart home is debatable, but it gives a broader over-view of a futuristic home. Today's smart home are composed of sensors that can feel, talk among themselves and to the user, act upon itself or on command of the user and thereby making the life comfortable. However, the key challenges in designing a smart home are ease of use, security aspect, access control , privacy issues and cost of deployment (Bugeja, Jacobsson, & Davidsson, 2016; Zhang, Adhikari, Pipattanasomporn, Kuzlu, & Rahman, 2016).

The goal of this paper is two-fold: Firstly, we are addressing the security aspect and access control of smart home by employing third party authentication mechanism. Secondly, minimizing the cost of deployment, by using the existing home infrastructure where most of the electronic appliances aren't "smart" i.e. they don't have networking capabilities.

The current trends on implementing security in smart home are using key exchanges and use of certificates and access control mechanism (Agosta, Antonini, Barenghi, Galeri, & Pelosi, 2015; Chitnis, Deshpande, & Shaligram, 2016). The smart home appliances manufactured by vendors uses their own industrial securities protocols (European Union Agency for Network and Information Secu-

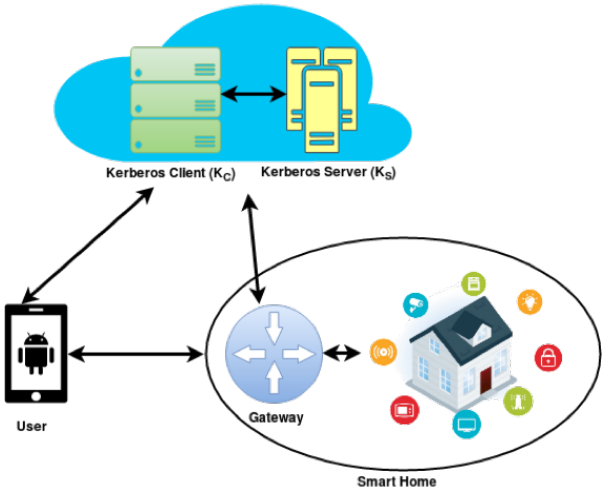


Figure 1. Smart home architecture / Arquitectura de una casa inteligente

I. Introducción

Los hogares inteligentes se están convirtiendo cada vez más en una tendencia en el estilo de vida moderno. Un hogar confortable es fuente de felicidad, salud y buena conciencia en la vida humana. El desarrollo de las Tecnologías de la Información y la Comunicación [TIC] lleva a las casas a un nivel completamente nuevo donde, un hogar puede "sentir", aprender y pensar por sí mismo.

El hogar aprende los hábitos de la persona que vive allí y actúa acorde con ello. A pesar de que esta definición de hogar inteligente es discutible, ofrece una visión general más amplia de un hogar futurista. Las casas inteligentes de hoy en día se componen de sensores que pueden sentir, hablar –entre ellos y con el usuario–, actuar por sí mismos o bajo el control del usuario y, por lo tanto, hacer que la vida sea cómoda. Sin embargo, los desafíos clave en el diseño de un hogar inteligente son: la facilidad de uso, los aspectos de seguridad, el control de acceso, los problemas de privacidad y el costo de implementación (Bugeja, Jacobsson, & Davidsson, 2016; Zhang, Adhikari, Pipattanasomporn, Kuzlu, & Rahman, 2016).

El objetivo de este documento es doble: en primer lugar abordamos el aspecto de seguridad y el control de acceso al hogar inteligente empleando un mecanismo de autenticación de terceros; en segundo lugar buscamos minimizar el costo de su implementación, usando la infraestructura existente en el hogar, donde la mayoría de los dispositivos electrónicos no son "inteligentes", es decir, no tienen capacidades de red.

Las tendencias actuales en la implementación de seguridad en el hogar inteligente están utilizando intercambios de clave y el uso de certificados y mecanismos de control de acceso (Agosta, Antonini, Barenghi, Galeri, & Pelosi, 2015; Chitnis, Deshpande, & Shaligram, 2016). Los electrodomésticos inteligentes fabricados por proveedores utilizan sus propios protocolos industriales de seguridad (European Union Agency for Network and Information Security, 2015; "Your home...", 2017; "hue: Your...", 2017). Sin embargo, la mayoría de estos enfoques son de naturaleza teórica o funcionan en redes privadas.

En este documento proponemos utilizar una herramienta de autenticación de terceros implementada en la nube para verificar las credenciales de un usuario, proporcionar un inicio de sesión único para acceder a los electrodomésticos inteligentes. Nuestra implementación está destinada a acceder a la casa inteligente de forma remota a través de Internet. Esto puede ser necesario, no solo para los residentes, sino también para otros, como el sensor de detección de incendios del Departamento de Bomberos o vigilancia.

Nuestra casa inteligente está compuesta de tres módulos (**Figura 1**): el módulo de dispositivos o electrodomésticos, que se compone de todos los sensores y aparatos en una casa inteligente; el módulo de seguridad, que se preocupa del acceso de los usuarios al sistema; y el módulo de aplicación, que se utiliza para monitorear y controlar los dispositivos inteligentes.

Nuestra arquitectura se puede integrar fácilmente a la infraestructura existente. Desde el punto de vista del proveedor de servicios para el hogar inteligente, el modelo económico, y los derechos de acceso a los diferentes usuarios de la casa inteligente se pueden implementar fácilmente. El acceso restringido puede ser necesario para el huésped o puede ser emitido para monitorear el sensor de incendios por el Departamento de Bomberos y, por su parte, la placa de transmisión de energía puede monitorear el medidor inteligente. Por otro lado, la implementación de la puerta de enlace y la capa de percepción también es muy fácil. Hemos implementado la puerta de enlace en DragonBoard 410c y conectado aparatos como una bombilla o conectividad de potencia de ventilador directamente a ella. Para conectar el refrigerador o el aire acondicionado es posible que se necesiten algunas modificaciones que permitan conectar el controlador integrado con la puerta de enlace.

El resto del trabajo se describe a continuación: en la Sección 2 se brinda una descripción general de los trabajos relacionados en el campo del hogar inteligente; en la sección 3, se presenta la arquitectura de hogar inteligente propuesta; en la sección 4 su implementación; en la sección 5 la evaluación experimental del modelo propuesto; y en la sección 6 las conclusiones.

II. Trabajos relacionados

La tecnologíadel Internet de las Cosas [IoT] impulsó el desarrollo de hogares inteligentes (Hosek, Masek, Kovac, Ries, & Kröpfl, 2014; Kubitza, Voit, Weber, & Schmidt, 2016). La inteligencia del hogar ahora está modificando la tendencia: de ser un sirviente a ser un mayordomo, es decir, el hogar ahora puede aprender y pensar por sí mismo y cuidar a su amo (Chen et al., 2017).

La confiabilidad de un hogar inteligente depende, en gran medida, de su fuente de alimentación, por lo que es necesario un estudio exhaustivo de la energía compleja al interconectar diferentes módulos para inducir la inteligencia en el hogar (Saurugg & Pichlmayr, 2013).

Los beneficios de las casas inteligentes conectadas dan lugar a nuevos paradigmas sobre problemas de seguridad. En el pasado, los residentes estaban preocupados principalmente por el robo fisico en su hogar, ahora con todos estos dispositivos conectados, surge la posibilidad de robo digital de una casa inteligente. El análisis de los riesgos actuales en los hogares inteligentes se realiza en Fernandes, Jung, y Prakash (2016) y en Jacobsson, Boldt y Carlsson (2016). El estudio de las medidas de seguridad se compila en Wendzel (2016); Ho, Leung, Mishra, Hosseini, Song y Warner (2016); y Holzleitner y Reichl (2017).

III. Arquitectura

El enfoque principal de artículo consiste en diseñar una casa inteligente segura utilizando la infraestructura existente. La mayoría de los electrodomésticos no tienen ninguna capacidad de conexión en red. Es costoso actualizar estos dispositivos para hacerlos "inteligentes" y conectarlos a una red. Con el propósito de resolver el problema de red, utilizamos una puerta de enlace que está conectada

rity, 2015; "Your home...", 2017; "hue: Your...", 2017). However, most of these approaches are theoretical in nature and/or works in private network. However, in this paper, we are proposing use of third party authentication tool deployed in cloud to verify the credentials of a user, provide a single sign-on and his/her access to the smart home appliances. Our implementation is intended to access the smart home remotely via internet. This may be required not only for the residents but may also be important for other parties like monitoring of fire detecting sensor by fire department or in surveillance also.

Our smart home is composed of three modules (**Figure 1**). The appliance module that is composed of all the sensor and appliance in a smart home. Security module is concerned with user access to the system. Finally the application module is use by the user to monitor and control the smart devices.

Our architecture can be easily integrated in existing infrastructure. From the smart home service provider view, the economic model, access rights to different users of the smart home can be easily implemented. Restricted access may be needed for guest, or it may be issued to monitor the fire sensor by fire department and power transmission board can monitor the smart meter. Deploying gateway and perception layer is also very easy. We deployed the gateway on DragonBoard 410c and connect appliances like a bulb or fan power connectivity directly to it. To connect refrigerator or air conditioner, some modification may be needed to connect their in-built controller with the gateway.

The rest of the paper is as follows. Section 2 gives an overview of related works in field of smart home. In section 3, we present our proposed architecture of smart home and implementation in section 4. The experimental evaluation of the proposed model is done in section 5. The paper is concluded in section 6.

II. Related works

Internet of Things [IoT] technologies are driven force in the development of smart homes (Hosek, Masek, Kovac, Ries, & Kröpfl, 2014; Kubitza, Voit, Weber, & Schmidt, 2016). The smartness of home is now changing trends from being a servant to a butler i.e. the home can now learn and think on its own and take care of its master (Chen et al., 2017).

The reliability of a smart home heavily depends upon the power supply, so a comprehensive study of complex power is must while interconnecting different modules to induce the smartness in the home (Saurugg & Pichlmayr, 2013).

The benefits of connected smart homes give rise to several new paradigms of security issues. In past, the residents were mainly concerned about physical theft in their home, now with all these connected devices, the digital burglary from a smart home emerged. Analysis of current risks in smart homes is done in (Fernandes, Jung, & Prakash, 2016; Jacobsson, Boldt, & Carlsson, 2016). Study of security measures are compiled in Wendzel (2016), Ho, Leung, Mishra, Hosseini, Song and Warner (2016) and Holzleitner and Reichl (2017).

III. Architecture

The main focus of this paper is designing a secure smart home using existing infrastructure. Most electrical appliances do not have any networking capability. It's a costly affair to upgrade these devices in order to make them ``smart'' and connect them to a network. To resolve the networking issue, we use a gateway that is directly connected to all the appliances and can control them. To address the security aspect of smart home, we considered use of third party single sign-on authentication tool. By using a third party tool, the development cost is minimized, as these tools are already tested against various security attacks. The single sign-on is convenient because the user does not need to enter the user-name and password, each time he/she wants to sign in to the system and can access the system for stipulated time.

Our smart home architecture consists of three different modules as follows:

- Appliance module: This module constitutes of all the appliances like bulb, fan, air conditioner, refrigerator and sensors like fire detection sensor. Most of the devices don't have networking capabilities.
- Security module: The security module validates a user and provides access privileges for accessing the devices. For example, the fire department can only access the fire detector sensor. Although, there are many third party authentication tools like SAML (“Single sign-on...”, 2017), WebAuth (“IT Services...”, 2017) and Kerberos ("Kerberos: The...", 2017) are present. In our implementation we are using Kerberos to authenticate the user.

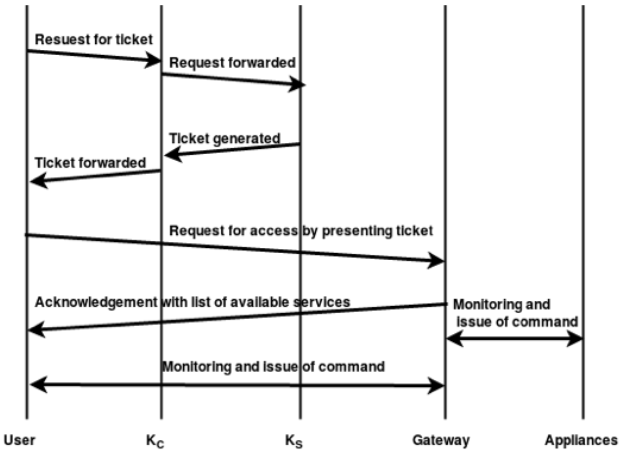


Figure 2. Timing diagram of smart home / Diagrama de tiempo de la casa inteligente

directamente a todos los dispositivos y puede controlarlos. Para abordar el aspecto de seguridad de la casa inteligente, consideramos el uso de una herramienta de autenticación de inicio de sesión único de terceros. Al utilizar una herramienta de terceros, el costo de desarrollo se reduce al mínimo, ya que estas herramientas están probadas contra varios ataques de seguridad. El inicio de sesión único es conveniente porque el usuario no necesita ingresar el nombre de usuario y la contraseña cada vez que desee iniciar sesión en el sistema; además, puede acceder al sistema por el tiempo estipulado.

Nuestra arquitectura de hogar inteligente consta, como se indicó, de tres módulos diferentes como se presenta a continuación.

- Módulo de electrodomésticos, compuesto por todos los dispositivos (como bombilla, ventilador, aire acondicionado, refrigerador) y sensores (como el detector de incendios). La mayoría de los dispositivos no tienen capacidades de red.
- Módulo de seguridad, que valida a los usuarios y les proporciona (o limita) privilegios de acceso a los dispositivos (por ejemplo, el Departamento de Bomberos solo puede acceder al sensor del detector de incendios. Aunque hay muchas herramientas de autenticación de terceros como SAML ("Single sign-on ...", 2017), WebAuth ("IT Services ...", 2017) y Kerberos ("Kerberos: The ...", 2017), en nuestra implementación usamos Kerberos.
- Módulo de aplicación, que proporciona una interfaz para que el usuario pueda supervisar y controlar los dispositivos de su hogar inteligente, para lo cual se desarrolló una aplicación basada en Android.

El funcionamiento de la arquitectura propuesta se muestra en el diagrama de tiempos de la **Figura 2**. El usuario solicita al KC que se ponga en contacto con KS para proporcionar un ticket. Tras la verificación exitosa de las credenciales del usuario por parte de KS, se genera un ticket y se envía a KC. KC luego reenvía este ticket al usuario. El

usuario presenta el ticket a la puerta de enlace de la casa inteligente y, al autenticarlo con éxito, reconoce al usuario con una lista de los servicios que se le ofrecen. La lista de servicios depende de los privilegios de acceso.

IV. Implementación

La implementación de nuestra arquitectura se compone de dos pasos diferentes: implementar Kerberos en la nube; e instalar la puerta de enlace en el hogar y conectar todos los dispositivos a ella, como se explica a continuación.

A. Implementación de kerberos

La implementación de Kerberos en la nube la realiza el proveedor de servicios de la casa inteligente. Smart Home puede ser un servicio proporcionado por un proveedor de servicios. Al igual que la instalación del enrutador para una conexión a Internet de banda ancha, el proveedor de servicios domésticos inteligentes instala la puerta de enlace y la conecta a la nube.

Para acceder a la puerta de enlace, el usuario necesitaría un tiquete generado por Kerberos Server [KS]. La puerta de enlace kerberized valida este ticket y lo descifra con su propia clave privada. El detalle del control de acceso también se proporciona en el tiquete emitido utilizando el servicio del Protocolo ligero de acceso a directorios [LDAP].

La validez del tiquete también es una característica importante. El tiquete del usuario debe renovarse diariamente para evitar cualquier inconsistencia con respecto a la duplicación del tiquete emitido. Por otro lado, un tiquete emitido al departamento de bomberos puede tener una validez de 365 días.

Un problema desafiante en esta arquitectura es el uso de Kerberos. Éste generalmente se usa en redes empresariales y no se puede acceder a través de Internet. Se recomienda que el sistema en el que se implementa el servidor Kerberos no ejecute ningún otro proceso. Para resolver este problema, utilizamos Kerberos Client [KC]. KS es el servidor real en el que se implementa Kerberos y no es visible para el mundo exterior. KC, que también se implementa en la nube, es visible para el público y está conectado a KS internamente. KC realmente proporciona un puente entre el usuario y KS. El usuario envía sus credenciales a KC, que las envía a KS. KS autentica al usuario y genera el tiquete requerido y lo envía de vuelta a KC, el cual confirma la devolución del usuario con el tiquete generado.

B. Instalación de la puerta de enlace

La puerta de enlace es el punto de interacción entre el usuario y el hogar inteligente. Hemos utilizado el tablero DragonBoard 410c para fines de implementación y hemos conectado los aparatos eléctricos como el ventilador y la bombilla usando una placa de prueba. DragonBoard funciona con Linaro OS (basado en Debian) y python se usa para implementar el programa de toma de corriente con fines de comunicación y acceder a los pines de entrada / salida de propósito general [GPIO] de DragonBoard.

- Application module: The application module is to provide an interface for the user to monitor and control appliances of his/her smart home. We developed Android based application for this module.

The working of the proposed architecture is shown by the timing diagram in **Figure 2**. The user requests the KC to contact KS for providing a ticket. Upon successful verification of user's credentials by KS, a ticket is generated, and sent to KC. KC then forwards this ticket to the user. The user present the ticket to gateway of smart home, and on successful authentication, acknowledge the user with a list of services offered to him /her. The list of services depends upon the access privileges.

IV. Implementation

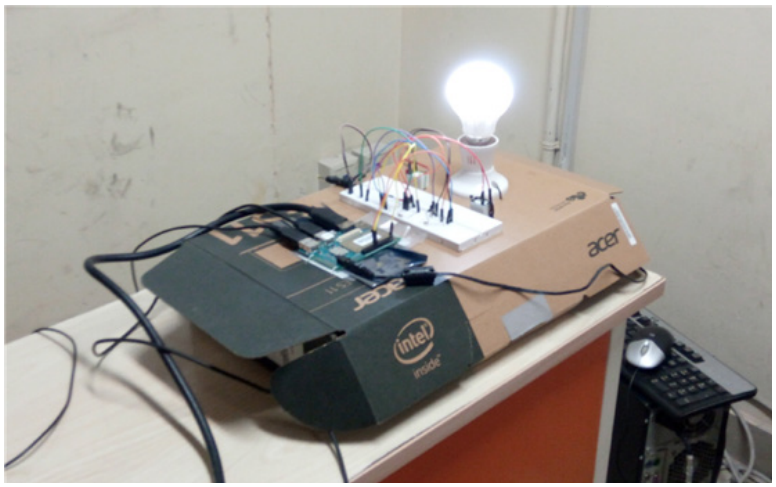
The implementation of our architecture consists of two different steps. First is to deploy Kerberos in the cloud and second is to install the gateway in the home and connect all the appliances to it, as discussed below:

A. Deployment of kerberos

The deployment of Kerberos in cloud is done by the service provider of smart home. Smart home can be a service provided by service provider. Just like installation of router for a broadband internet connection, the smart home service provider installs the gateway and connect it to the cloud. To access the gateway, the user required a ticket generated by Kerberos Server [KS]. The kerberized gateway validates this ticket by decrypting with its own private key. The access control detail is also provided in the issued ticket using Lightweight Directory Access Protocol [LDAP] service. The validity of the ticket is also an important feature. The user's ticket has to be renewed on daily basis, to avoid any inconsistencies regarding duplication of issued ticket. On the other hand, a ticket issued to fire department can have a validity of 365 days.

A challenging issue in this architecture is use of Kerberos. Kerberos is generally use in enterprise networks and cannot be accessed through the internet. It is advised that the system on which Kerberos server is implemented should not run any other process. To resolve this issue, we use and Kerberos Client [KC]. KS is the actual server on which Kerberos is implemented and is not visible to outside world. KC which is also implemented in cloud is visible to public and is connected to KS internally. KC actually provides a bridge between the user and KS. The user sends his/her credentials to KC, which forwards

A)



B)

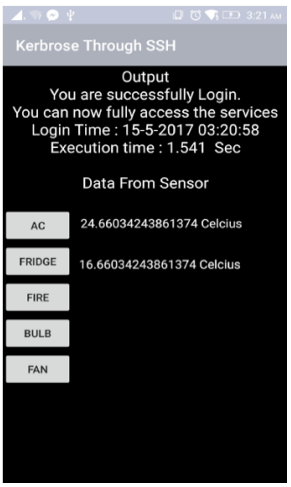


Figure 3. Smart home evaluation: experimental Setup (a); Smart home application (b) / Evaluación de la casa Inteligente: configuración experimental (a); aplicación de la casa inteligente (b)

them to KS. KS authenticates the user and generates the required ticket and sent it back to KC, which acknowledges back the user with the generated ticket.

B. Installation of Gateway

The gateway is the point of interaction of the user and smart home. We have used DragonBoard 410c board for implementation purpose and connect the electrical appliances like fan and bulb using breadboard. The DragonBoard is powered by Linaro OS (Debain based) and python is used to implement the socket program for communication purpose and accessing General-Purpose Input/Output [GPIO] pins of the DragonBoard. The GPIO pins are used to switch on/off appliances. The gateways maintains a database of every appliance and the GPIO pin in the smart home. The gateway is kerberized and has a public IP address. The public IP is used by the user to connect to the gateway. The private key of gateway is stored in KS. When the user login for the first time by presenting the ticket issued by KS, the gateway decrypts the ticket using its own private key. The ticket is also time stamped, which is a functionality of Kerberos that disallows replay attacks.

Apart from providing secure access and controlling the devices upon user request, an important feature of the gateway is to make the appliances talk to each other. Most of the devices used in smart homes use different modes of communication like Bluetooh, WiFi, Zigbee and other industrial communication technologies. Some of these devices, as in our implementation even lacks networking capabilities. In order to enable communication among them and thus provide better services for residents of the smart home, the gateway acts as a central entity to facilitate communication among them.

Los pines GPIO se utilizan para encender / apagar los dispositivos.

Las puertas de enlace mantienen una base de datos de cada dispositivo y el pin GPIO en la casa inteligente. La puerta de enlace es Kerberized y tiene una dirección IP pública, la cual es utilizada por el usuario para conectarse a la puerta de enlace. La clave privada de la puerta de enlace se almacena en KS.

Cuando el usuario inicia sesión por primera vez, presentando el tiquete emitido por KS, la puerta de enlace descifra el tiquete usando su propia clave privada. El tiquete también tiene un sello de tiempo, una funcionalidad de Kerberos que evita ataques de repetición.

Además de proporcionar acceso seguro y controlar los dispositivos a petición del usuario, una característica importante de la puerta de enlace facilitar la comunicación entre sí de los dispositivos. La mayoría de los dispositivos utilizados en hogares inteligentes utilizan diferentes modos de comunicación, como Bluetooh, WiFi, Zigbee y otras tecnologías de comunicación industrial. Algunos de ellos, como es en caso en nuestra implementación, carecen de capacidades de red. Con el fin de permitir la comunicación entre ellos y así proporcionar mejores servicios para los residentes de la casa inteligente, la puerta de enlace actúa como una entidad central para facilitar la comunicación entre ellos.

V. Resultados experimentales

Para evaluar el rendimiento de la arquitectura propuesta, realizamos múltiples experimentos utilizando dispositivos reales. Conectamos una bombilla y un ventilador directamente a la DragonBoard mientras simulamos el aire acondicionado y el refrigerador (**Figura 3a**). La simulación se realiza mediante un programa Java que modifica ambas temperaturas a intervalos regulares. La puerta de enlace lee estos valores cada 10 segundos para que el usuario pueda monitorearlos en tiempo real. Aseguramos la comuni-

cación segura del usuario con KC y la puerta de enlace, igualmente utilizamos la tecnología de seguridad Secure Socket Layer [SSL]. La transferencia del tiquete se realiza utilizando Secure Shell [SSH].

También realizamos experimentos utilizando un http seguro [HTTPS]. Se mantiene una base de datos de usuarios en KC, mientras que la información del tiquete, la clave privada del usuario y la puerta de enlace se almacenan en KS. La evaluación del sistema se lleva a cabo investigando el tiempo empleado por el usuario para iniciar sesión en la casa inteligente y emitiendo comandos para activar / desactivar la bombilla usando los protocolos HTTPS y SSH. Desarrollamos una aplicación basada en Android para facilitar el monitoreo y el control de los electrodomésticos inteligentes (**Figura 3b**). El tiempo de ejecución, que es 1.541 segundos, es el tiempo empleado en adquirir el tiquete de KS y el inicio de sesión en la puerta de enlace de la casa inteligente.

El tiempo invertido en adquirir el tiquete de Kerberos por usuario, utilizando el protocolo SSH en múltiples experimentos, se muestra en la **Figura 4**. El tiempo total dedicado para verificar las credenciales de usuario por Kerberos y acceder a la puerta de enlace se muestra en la **Figura 5**. También calculamos el tiempo empleado en la ejecución un comando emitido por el usuario para operar un dispositivo en la casa inteligente. Los resultados se muestran en la **Figura 6**.

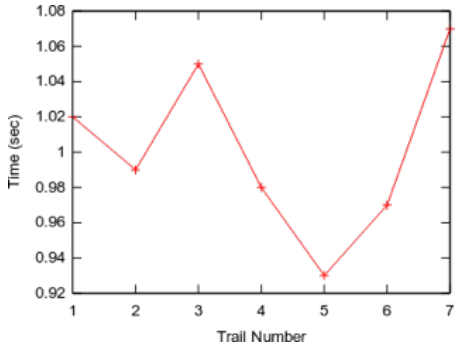


Figure 4. Time spent in acquiring ticket from Kerberos / Time dedicado para adquirir el tiquete de Kerberos

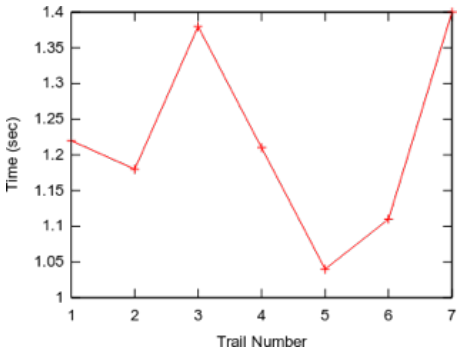


Figure 5. Total time spent in accessing gateway / Tiempo total dedicado para acceder a la puerta de enlace

V. Experimental results

To evaluate the performance of proposed architecture, we performed multiple experiments using real devices. We connect a bulb and a fan directly to the DragonBoard while simulated air conditioner and refrigerator (**Figure 3a**). The simulation is done by java program that keeps on changing both temperatures at regular intervals. The gateway reads these value every 10 second, so that the user can monitor it in real-time. The ensure secure communication of user with KC and gateway, we use Secure Socket Layer [SSL] security technology. The transfer of ticker is done using Secure Shell [SSH]. We also performed experiments using Hypertext Transfer Protocol Secure [HTTPS] protocol. A database of users is maintained in KC, while the ticket information, private key of user and gateway is stored in KS. The evaluation of the system is performed by investigating time spent in logging to the smart home by the user, issuing commands to switch on/off bulb using HTTPS and SSH protocols. We developed Android based application to facilitate monitoring and controlling the smart home appliances (**Figure 3b**). The execution time which is 1.541 second is time spent in acquiring ticket from KS and logging to the smart home gateway. Time spent is acquiring ticket from Kerberos by user using SSH protocol is in multiple experiments is shown in **Figure 4**. The total time spent in verifying credentials of user by Kerberos and accessing the gateway is shown in **Figure 5**. We also calculated time taken in executing a command issued by the user to operate an appliance in the smart home. The results are shown in **Figure 6**.

VI. Conclusions

In this paper, we present a secure smart home concept using third part authentication tool for verification of the user identity and access privileges. The proposed archi-

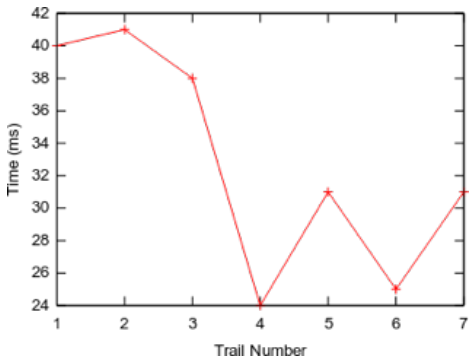


Figure 6. Time spent in operating an appliance / Tiempo dedicado para operar un electrodoméstico

tecture use existing household electrical appliances which lacks networking and processing power. It is a very practical approach in converting a home into a connected and intelligent smart home with very low deployment cost. The user can access and control the smart home appliances from anywhere using internet. Experiments on prototype of proposed smart home suggests that the time spent in authenticating the user is about 1.2 second and execution time of commands by user to control the appliances is on average 30 ms. ST

VI. Conclusiones

Presentamos un concepto de hogar inteligente seguro utilizando una herramienta de autenticación de terceros que verifica la identidad del usuario y sus privilegios de acceso. La arquitectura propuesta utiliza electrodomésticos existentes sin capacidad de red y procesamiento. Este es un enfoque muy práctico, que busca convertir una casa normal en una casa inteligente con un costo de implementación muy bajo.

El usuario puede acceder y controlar los electrodomésticos inteligentes desde cualquier lugar a través de Internet. Los experimentos en el prototipo de hogar inteligente propuesto sugieren que el tiempo dedicado a la autenticación del usuario sea de aproximadamente 1,2 segundos y el tiempo de ejecución de los comandos por parte del usuario para controlar los dispositivos consuman en promedio 30 ms. ST

References / Referencias

Agosta, G., Antonini, A., Barenghi, A., Galeri, D., & Pelosi, G. (2015). Cyber-security analysis and evaluation for smart home management solutions. In *2015 International Carnahan Conference on Security Technology (ICCST).* http://dx.doi.org/10.1109/ccst.2015.7389663

Bugeja, J., Jacobsson, A., & Davidsson, P. (2016). On privacy and security challenges in smart connected homes. In *2016 European Intelligence And Security Informatics Conference (EISIC).* http://dx.doi.org/10.1109/eisic.2016.044

Chen, S., Liu, T., Gao, F., Ji, J., Xu, Z., & Qian, B. et al. (2017). Butler, not servant: A human-centric smart home energy management system. *IEEE Communications Magazine, 55*(2), 27-33. http://dx.doi.org/10.1109/mcom.2017.1600699cm

Chitnis, S., Deshpande, N., & Shaligram, A. (2016). An investigative study for smart home security: Issues, challenges and countermeasures. *Wireless Sensor Network, 8*(4), 61-68. http://dx.doi.org/10.4236/wsn.2016.84006

European Union Agency for Network and Information Security [ENISA]. (2015). *Security and resilience of smart home environments good practices and recommendations.* Heraklion, Greece: ENISA.

Fernandes, E., Jung, J., & Prakash, A. (2016). Security analysis of emerging smart home applications. In *2016 IEEE Symposium on Security And Privacy (SP).* http://dx.doi.org/10.1109/sp.2016.44

Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D., & Wagner, D. (2016). Smart locks. *In Proceedings Of The 11Th ACM on Asia Conference on Computer and Communications Security - ASIA CCS '16.* http://dx.doi.org/10.1145/2897845.2897886

Holzleitner, M., & Reichl, J. (2017). European provisions for cyber security in the smart grid – an overview of the NIS-directive. *E&I, Elektrotechnik und Informationstechnik, 134*(1), 14-18. http://dx.doi.org/10.1007/s00502-017-0473-7

Hosek, J., Masek, P., Kovac, D., Ries, M., & Kröpfl, F. (2014). IP home gateway as universal multi-purpose enabler for smart home services. *E&I, Elektrotechnik und Informationstechnik, 131*(4-5), 123-128. http://dx.doi.org/10.1007/s00502-014-0209-x

hue: Your personal wireless lighting system. (2017). Retrieved 12 July 2017, from http://www2.meethue.com/en-in/about-/

IT Services: Stanford WebAuth. (2017). Webauth.stanford.edu. Retrieved 13 July 2017, from http://webauth.stanford.edu

Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. *Future Generation Computer Systems, 56,* 719-733. http://dx.doi.org/10.1016/j.future.2015.09.003

Kerberos: *The network authentication protocol.* (2017). Retrieved from https://web.mit.edu/kerberos

Kubitza, T., Voit, A., Weber, D., & Schmidt, A. (2016). An IoT infrastructure for ubiquitous notifications in intelligent living environments. In *Proceedings of The 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing Adjunct - Ubicomp '16.* http://dx.doi.org/10.1145/2968219.2968545

SAML Single Sign-On Solutions - SAML SSO Identity Provider, SAML Service Provider. (2017). Retrieved from https://www.onelogin.com/saml

Saurugg, H. & Pichlmayr, J. (2013). "Smart", vernetzung und komplexität – ein plädoyer für einen kritischeren umgang mit dem thema vernetzung. *E&I, Elektrotechnik Und Informationstechnik, 130*(4-5), 103-108. http://dx.doi.org/10.1007/s00502-013-0139-z

Wendzel, S. (2016). How to increase the security of smart buildings? *Communications of the ACM, 59*(5), 47-49. http://dx.doi.org/10.1145/2828636

Your home may be smart, but is it intelligent? It can be with IBM Watson IoT and cognitive computing. (2017). Retrieved from https://www.ibm.com/internet-of-things/iot-zones/iot-home/

Zhang, X., Adhikari, R., Pipattanasomporn, M., Kuzlu, M., & Rahman, S. (2016). Deploying IoT devices to make buildings smart: Performance evaluation and deployment experience. In *2016 IEEE 3Rd World Forum on Internet of Things (WF-IoT).* http://dx.doi.org/10.1109/wf-iot.2016.7845464

CURRICULUM VITAE

Amit Banerjee, Ph.D Assistant Professor at the Department of Computer Science of South Asian University (New Delhi, India) He received a Ph.D. in Computer Science from National Tsing-Hua University (Taiwan, 2009). He has a Masters' degree (MCA) in 2002 and B.Sc. Mathematics (Hons.) in 1998 from Visva Bharati University (India). He worked for two years as an engineer with SoC Technology Center, Industrial Technology Research Institute [ITRI] (Taiwan). His research interests include Wireless Adhoc and Sensor Networks, P2p networks / Profesor asistente del Departamento de Ciencias de la Computación de la South Asian University (New Delhi, India). Recibió su Ph.D. en Ciencias de la Computación de National Tsing-Hua University (Taiwan, 2009), y su MCA (2002) y su título en matemáticas (1998) de Visva Bharati University (India). Trabajo durante dos años como ingeniero en SoC Technology Center, Industrial Technology Research Institute [ITRI] (Taiwan). Sus áreas de interés en investigación incluyen redes inalámbricas Adhoc, sensoriales y entre pares (P2P).

Mohd Sameen Chishti, MCA Ph.D., student and research scholar at the Faculty of Mathematics and Computer Science of South Asian University (New Delhi, India). He obtained his masters' degree (MCA) in 2010 from Jamia Millia Islamia / Estudiante de doctorado y becario de investigación en la Facultad de Matemáticas y Ciencias de la Computación de la South Asian University (New Delhi, India). Obtuvo su maestría en 2010 en Jamia Millia Islamia.

Sunjai Kumar, MSc Ph.D., Researcher in programming languages, software engineering and computer communications (networks) at the Faculty of Mathematics and Computer Science of South Asian University (New Delhi, India) / Investigador en lenguajes de programación, ingeniería de software y redes en la Facultad de Matemáticas y Ciencias de la Computación de la South Asian University (New Delhi, India).