Integration of Multi Access Control System with Door, Device & Location Automation & Remote Network Control

Ms. J. S. Vimali,
Assistant Professor
Departmentt of Information Technology,
Sathyabama Institute of Science and Technology, Chennai.
vimali.it@sathyabamauniversity.ac.in

Abstract — **Android is the most popular mobile operating system currently developed by Google, based on the Linux kernel. It is open source, thus the Operating System itself can be ported to different categories of devices like Watches (Wearables), Cars (Auto), TV, Gaming Consoles etc. The current devices are packed with all kinds of sensors and data collection abilities, users also store their personal information on the device. The project aims at bringing all the access controls at user's finger tips on his/her Android device.It can be used to switch on/off home appliances like lights, fans, etc. via the Bluetooth module (HC-05). The Application connects to a LAN Network of PC, and is able to Shutdown, Restart or Log off the PC in the LAN Network. In order to perform these remote tasks, the application makes use of Java RMI (Remote Method Invocation).Java RMI, is based on the Stub/Skeleton technology.**

Keywords— Android, ABE, Microcontroller, RMI, Bluetooth.

1. Introduction

The widespread availability of wireless network connectivity in the environments where users live and work together with the increasing diffusion of portable devices creates novel opportunities for users to access services anywhere, at any time and from various access devices. In particular, mobile users/devices can have access not only to traditional Internet services, designed and implemented for the fixed network infrastructure, but also to new classes of services that can provide results depending on the relative position of clients and on the consequent resource visibility. However, the design and deployment of ubiquitous services lead to serious security risks and access control problems and impose new challenges to the secure retrieval and operation on distributed resources, undermining several assumptions of traditional security solutions. Traditional solutions typically evaluate permissions depending on the identity/role of the client requesting access to resources. However, the new ubiquitous scenario makes service providers deliver services often to unknown entities and, more important, whose identity may be un-informative or not sufficiently trustworthy. In fact, it is almost impossible for service providers to know in advance the identities/roles of all subjects that are likely to request access to their managed resources/services.

Instead, service providers can more easily define the conditions for making resources available and for allowing/denying users' resource visibility and access according to the context operating conditions. In the following, we define context as the collection of any information useful to characterize the runtime situation of a user during her service session. Some initial research works are starting to recognize that ubiquitous service provisioning requires a paradigm shift from subject-centric to context-centric access control. Novel access control middleware solutions should consider context as a first-class principle to guide both policy specification and enforcement process. In this perspective, the changes in context should trigger the evaluation process of applicable permissions. Drawing inspiration from the RBAC model that exploits the concept of role as a mechanism for grouping subjects based on their properties, we state that, the same as with role, the concept of context can provide an indirection level between users and permissions. Instead of managing subjects and their permissions individually, a system administrator defines for each context the set of applicable permissions. When a subject operates in a specific context, she instantaneously acquires the set of permissions active for the related context. When she changes her operating context, her previous permissions are automatically revoked and the new permissions acquired.

2. Related Work

Michael Mitzenmacher, Yan-Cheng Chang, In their paper "privacy preserving keyword searches on remote encrypted data"[1] have offered a new solution in which no public key cryptography system is used and also their approach for remote files is independent from the encryption methods.

R. Ostrovsky, S. Kamara, J. Garay, and R. Curtmola, in their paper " Searchable Symmetric Encryption (SSE): Improved Definitions & Efficient Constructions"[2] proposed a new solution to the problems faced in a Searchable Symmetric Encryption system. The two solutions proposed by them are more efficient than the previous schemes. Both proposed schemes has a stronger guarantied security.

C. Hong, D. Feng, Min Zhang, ZhiquanLv, In their paper "Expressive & Secure Searchable Encryption in the Public Key Setting"[3] proposed a new encryption technique called ESASE scheme which stands for expressive & secure asymmetric searchable encryption. This encryption technique is the first one which supports disjunctive, negation and conjunctive search operations at the same time. This technique can also be used for multiple user profile setting as well as range search.

Charles Morisset, Jason Crampton, in their paper “An Auto-delegation Mechanism for Access Control Systems"[4] introduced a new delegation mechanism which is an automatic system and we can use this mechanism to provide controlled overriding and a unconventional access control mechanism. The mechanism used by this system is derive from subject object relationship.

P. Li, Y Tong, S.S. Chow, J Sun, in their paper “Cloud-assisted mobile-access of health data with privacy and auditability"[5] proposed to add privacy to the new generation mobile healthcare system by using the cloud technology. Their system has many key features like privacy protected data storage, effective key management technique and retrieval of lost data.

3. Proposed System

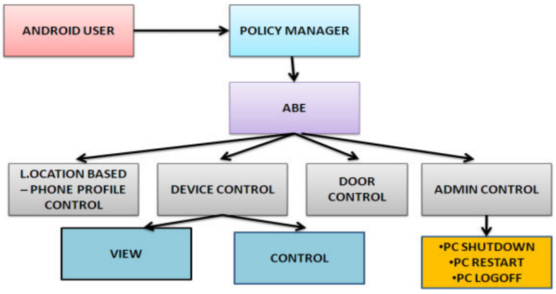

Figure 1. Architecture

The above diagram shows the flow of control of the system. ABE Algorithm is used to encrypt all the transactions happening in the system. The device control module has 2 modes. One of them gives only viewing privileges & other one lets the user control. This can be implemented in different locations and Location based phone profile control can be set to have individual control of each section from same device.

4. Implementation

4.1. Attribute Based Encryption [ABE]

Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. A crucial security aspect of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

The concept of attribute-based encryption was first proposed in a landmark work by Amit Sahai and Brent Waters and later by Vipul Goyal, Omkant Pandey, Amit Sahai and Brent Waters. Several researchers have further proposed Attribute-based encryption with multiple authorities who jointly generate users' private keys.

4.2. PC Control Module

The PC Control module consists of 2 sets of Java code that is based on the Java RMI Technology. The first set of code is the server-side code, which runs on 1 of the machines in the LAN Network. The second set of code is the client-side code, which runs on rest of the machines in the LAN Network, these client machines can controlled via our application on the Android device.

4.3. Remote Method Invocation

The **RMI** (Remote Method Invocation) is an API that provides a mechanism to create distributed application in java. The RMI allows an object to invoke methods on an object running in another JVM.The RMI provides remote communication between the applications using two objects *stub* and *skeleton*.RMI uses stub and skeleton object for communication with the remote object. A **remote object** is an object whose method can be invoked from another JVM. Let's understand the stub and skeleton objects:

The stub is an object, acts as a gateway for the client side. All the outgoing requests are routed through it. It resides at the client side and represents the remote object. When the caller invokes method on the stub object, it does the following tasks:

1. It initiates a connection with remote Virtual Machine (JVM),
2. It writes and transmits (marshals) the parameters to the remote Virtual Machine (JVM),
3. It waits for the result
4. It reads (un-marshals) the return value or exception, and
5. It finally, returns the value to the caller.

The skeleton is an object, acts as a gateway for the server side object. All the incoming requests are routed through it. When the skeleton receives the incoming request, it does the following tasks:

1.It reads the parameter for the remote method

2. It invokes the method on the actual remote object, and

3. It writes and transmits (marshals) the result to the caller.

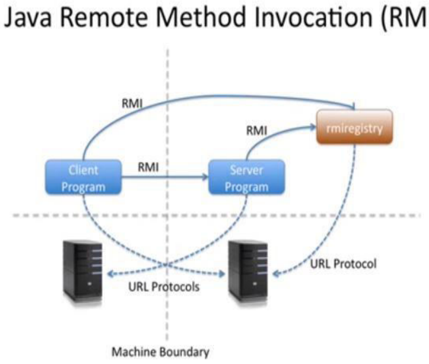

Figure 2. Java RMI Workflow

As java doesn't have access to low level commands like Shutdown, Restart and Log Off. The application makes use of the Java Runtime, which are executed in Command Prompt.

The commands used are "shutdown –s" for Shutdown, "shutdown –r" for Restart, "shutdown –l" for Log Off.

4.4. Bluetooth Switch Control Module

The Microcontroller being used here is PIC16F877 from Microchip. It is a 8-bit, 40 pin microcontroller.

Figure 3. PIC16F877A Microcontroller

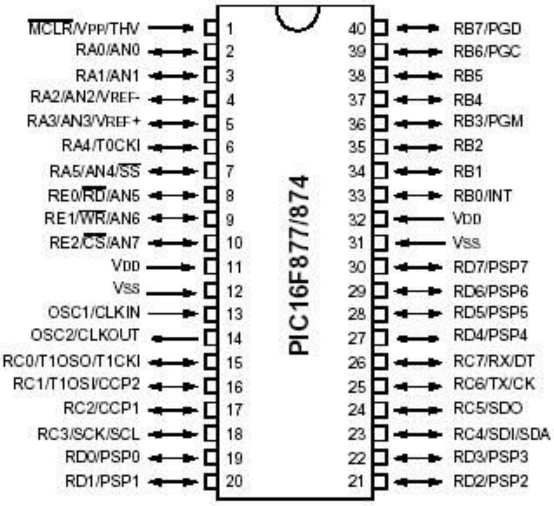

Figure 4. PIC16F877A PIN Diagram.

Bluetooth connection is used instead of widely used ZigBee(IEEE 802.15.4) as its security can be compromised.

The Bluetooth module integrated with microcontroller setup is HC-05.

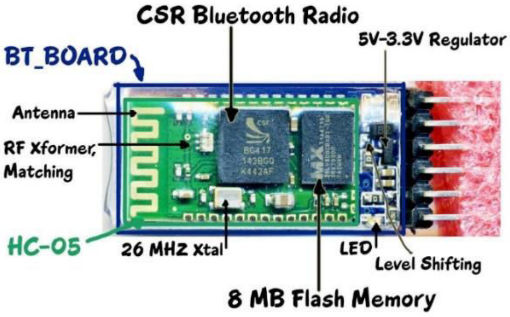

Figure 5. HC-05 BT Module

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). Range is approximately 10 Meters (30 feet).

These modules are based on the Cambridge Silicon Radio BC417 2.4 GHz Bluetooth Radio chip. This is a complex chip which uses an external 8 Mbit flash memory. These low-cost Bluetooth Sub-modules work well with Arduino and other Microcomputers.

- HC-05 is a more capable module that can be set to be either Master or Slave.
- HC-06 is a Slave only device. It looks physically just like the HC-05

- These small (3 cm long) modules run on 3.3V power with 3.3V signal levels, it has **no** pins and usually solder to a larger board.
- The module has two modes of operation, Command Mode where we can send AT commands to it and Data Mode where it transmits and receives data to another Bluetooth module.

"Breakout" Boards that make these easy to use are available and recommended. These mount the sub-module like that shown on the right on a slightly larger board. NOTE: Sellers often label them "HC-05" or "HC-06", but they have some other model number on the reverse side. Most of these boards support operation at 5V power and interface to 5V Arduino signal levels with some technique of level shifting.The board requires a 12 Volts supply, which can be battery powered or straight out of the powerline using an AC Adapter.Package used for programming “pic.h” the microcontroller board.

5. OUTPUT

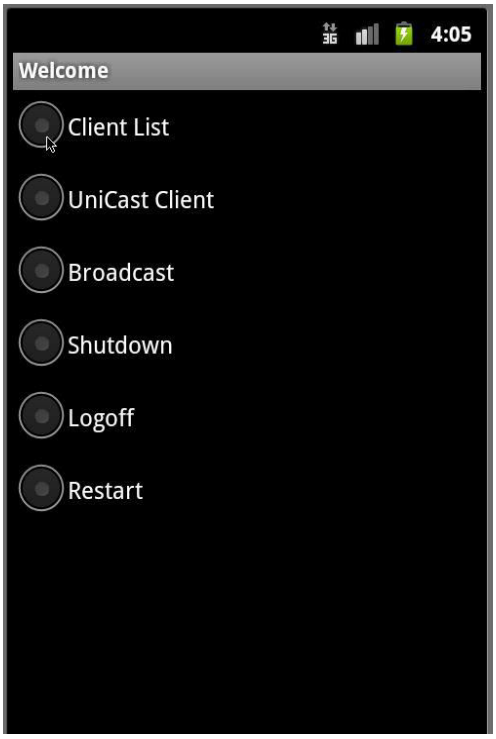

Figure 6. Admin Control Screen

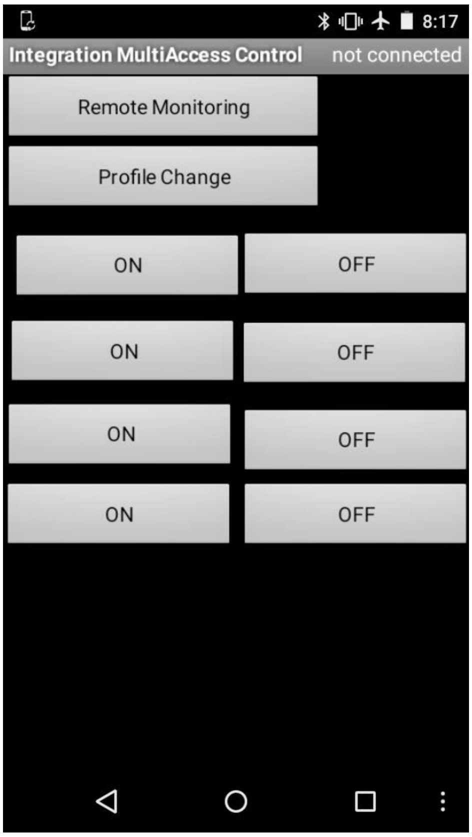

Figure 7. Switch Control

CONCLUSION

The implementation can be done easily as the modules are cost effective and portable. This workt wasn’t implemented in IOT [Internet of Things] because it’s current security issues and dangerous malwares available on the Web. As these security issues are resolved, this can be implemented in IOT. Custom designed microcontrollers can be used to improve the efficiency of the workload. The Client Java service can be integrated into Windows Services for better Admin Control on the Client machines.This whole circuit can be embedded directly into home electrical circuit for better efficiency and control.

ACKNOWLEDGEMENT

I wish to acknowledge the Department of Science and Technology, India and School of Computing, Sathyabama Institute of Science and Technology, Chennai for providing the facilities to do the research under the DST-FIST Grant Project No.SR/FST/ETI-364/2014.

REFERENCES

[1]. Chang YC, Mitzenmacher M., “Privacy Preserving Keyword Searches on Remote Encrypted Data”, Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science, Vol 3531. Springer.

[2]. Reza Curtmola, Juan Garay, Seny Kamara, RafailOstrovsky, “Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions”, https://eprint.iacr.org/2006/210.pdf

[3]. P. Vagdevi; Divya Nagaraj; Golla Vara Prasad, ”Home: IOT based home automation using NFC”, International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC - 2017), Pages: 861 – 865.

[4]. ZhiquanLv, Cheng Hong, Min Zhang, Dengguo Feng, “Expressive and Secure Searchable Encryption inthe Public Key Setting (Full Version)”, (https://eprint.iacr.org/2014/614.pdf).

[5]. Crampton J, Morisset C, “An Auto-delegation Mechanism for Access Control Systems”, Security and Trust Management. STM 2010. Lecture Notes in Computer Science, vol 6710, Springer.

[6]. Yue Tong, Jinyuan Sun, Sherman S. M. Chow, Pan Li, “Cloud-Assisted Mobile-Access of Health Data with Privacy and Auditability”, IEEE Journal of Biomedical and Health Informatics, Vol. 18, No. 2, March 2014.

[7]. J. Sun, C. Zhang, Y. Zhang, Y. Fang, “An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks”, “IEEE Transactions on Parallel and Distributed Systems” Vol. 21 , No. 9, 15 January 2010.

[8]. J. S Vimali, Z. Sabiha Taj, “FCM based CF: An efficient approach for consolidating big data applications”, International Conference Innovation Information in Computing Technologies (ICIICT -2015), DOI:10.1109/ICIICT.2015.7396090, IEEE.

[9]. R. Balamurali, J. S. Vimali, “ Certificate and message authentication acceleration in VANET“, International Conference Innovation Information in Computing Technologies (ICIICT -2015), DOI:10.1109/ICIICT.2015.7396089.