International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876; Impact Factor: RJIF 5.44
www.engineeringresearchjournal.com
Volume 2; Issue 2; March 2016; Page No. 67-71

Building a secure personal cloud on basic Infrastructure

[*1] Sushil Kumar, [2] Nilendu Ghosal, [3] Sheetal Srivastava

[1] Research Scholar, Maharaja Surajmal Institute of Technology New Delhi, India
[2, 3] Undergraduate Student, Maharaja Surajmal Institute of Technology, New Delhi, India

Abstract
Cloud computing provides architecture for an internet dependent on-demand service where the users can access a shared pool of resources such storage, network, servers and applications distributed across the globe in a cost effective manner. Just like with every rising technology, as emanate the benefits, so arise the security threats and cloud computing is no exception. The various security concerns associated with cloud computing are limited control over the data, access control management, data privacy, data integrity, data location and availability, network security, data security, virtual machine security etc. This paper primarily focuses on the essential theory of secure cloud computing by the implementation of a personal cloud server. This paper gives a briefing about the security threats in the current cloud environment and how these risks can be mitigated by a model of a personal cloud server.

Keywords: Cloud computing, security threats, personal cloud server, raspberry pi, raspbian OS, IoT application

Introduction

The notion of cloud has revolutionized the world of IT and Internet. It has paved new paths for research and development in the field of technology, business, and economics and is of growing importance in the industrial and scientific communities. Over the recent years, most if the data has been shifted to cloud.

A cloud can be seen as a conglomeration of physical resources distributed across the globe which can be accessed across the globe. One of the widely used definition of cloud computing as given by U.S. NIST (National Institute of Standards and Technology), "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

There are four types of cloud deployment models, namely: Private cloud, which is operated in a single organization, Public cloud, Community Cloud, Hybrid cloud. Furthermore, the three categories of cloud service models are: SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service).

The big giants in the cloud industry are Microsoft, Oracle, Google, and Amazon. Microsoft provides all three types of services. For PaaS itn includes. For SaaS, Office 365, Exchange server, sharepoint servers, and dynamic CRM. For IaaS, it provides Windows server and system center. The famous products by Google are Google Mail, Google docs (SaaS), Google AppEngine (PaaS) and by Amazon are Amazon EC2, and Amazon S3.

While cloud computing provides plethora of advantages like flexibility, work from anywhere, capital expenditure free, pay as much you use, disaster recovery and many more but it arises some serious security questions like where is this humungous amount of data getting stored, who all have access to this data, how many copies are getting made and of course how much secure and private is our data???

Apart from the existing cloud models (Public, Private, Hybrid and Community) we propose a personal cloud server model system which addresses the security issues of authentication, confidentiality and integrity.

Literature Review

According to a survey held in the year 2015 by kazim *et al* [5] the top security threats encountered in the present day cloud environment are as follows:

- Authentication
- Data accessibility
- Communication security
- Web security
- Network security
- Data protection
- Malicious s/w attack
- Shared resources

To address these security concerns, many authors have come up with their awe-inspiring research work in the field of cloud computing security. Some of which are as under:

In 2010, Cong Wang *et al*, proposed an effective Third Party Auditor (TPA) which will provide data storage security of cloud. They suggested the use of the public key based homomormic authenticators under the Privacy-Preserving Public Auditing Scheme [2].

In 2010, Zhidong proposed a design in which security functions such as data protection, authentication and communication security is provided by Trusted Cloud Platform (TCP). They used TCP as a secure base to achieve trusted cloud computing [3].

In 2015, Rajkumar come up with the idea of using Cloud Security Alliance (CSA) which will ensure the availability of cloud security tools and help the organizations to create public as well as private cloud [4]

To further enhance the solutions to the security threats of data availability, data location, data security, authentication and authorization etc., we propose a model for a Personal Cloud Server in which the above security threats will be

minimized and server portability will be provided.

Proposed Work

Keeping the main concept of security in mind, we devised our personal cloud server using Raspberry Pi and dedicated peripherals such as mouse, keyboard, monitor, Wi-Fi router etc. The main reason behind the choice of Raspberry pi is to provide portability to our cloud server. Raspberry Pi is a minicomputer, nearly the size of small credit card. Since, we have used Raspbian OS which is linux based hence making it implicitly immune to threats like viruses, worm etc. Features of the project will include *external storage for cloud data (with the help of a php script that will redirect the storage location of cloud data), secure login with OTP (ensured by an android app), wired as well as wireless access to the server, a platform for IoT Application development, decentralized data encryption with Tiny Algorithm Software based on Java*.

Steps taken to implement the idea will be covered in the upcoming sections.

Implementation

We can divide the implementation process into two parts:

A. Hardware Realization: To provide portability to the personal cloud server we use Raspberry pi." Raspberry Pi is a low cost credit card sized computer that plugs into a computer monitor or TV (now it has its own display unit) and uses a standard keyboard and mouse". We have used raspberry pi as CPU not as a microcontroller. It consists of 1GB RAM, ARM 7 Broadcom processor and operates at the speed of 1GHz. It supports both Linux and Windows environment. It has 4 USB ports, 1 Ethernet port, 40 GPIO's for external hardware interface, 1 HDMI port for display unit, 1 SD card slot, 1 port for dedicated display, 1 port for dedicated camera and 1 audio jack.

B. Software Realization: Many OS are available for Raspberry Pi like Ubuntu, NOOBS, Raspbian but we are using Raspbian OS as it is an open source operating system based on Debian which is a Linux distribution and optimized for the Raspberry Pi. Raspbian OS come with over 35,000 of pre-installed packages, pre-compiled software bundled in a nice format.

Since Raspbian OS is a Linux distribution, so it is highly unlikely to get attacked by viruses. Some of the famous viruses like Trojans which steal data from our PC has no effect on Raspbian OS hence making it secure.

Many packages are available for Raspbian OS but the packages required to be installed for personal cloud are as follows:

- **Apache2**: It is an open source HTTP server for secure file transfer, php-server-side scripting language for building web pages.
- **Php5-gd**: For adding image functionality in web pages.
- **SQLite**: For database management
- **Php5-sqlite**: To link the database with web pages.
- **Php5-curl:** Used for downloading files via HTTP or FTP with security and linking data with other websites.

For making the GUI or our personal cloud server, we have used php. The starting page contains the login and password which when entered correctly will give access to the cloud files. We have provided many facilities like making groups, sharing file with other users, etc. Since our cloud is for personal usage or for small organizations therefore we have given the admin permission to make users and groups so that unknown users can't create account on our cloud.

After making the GUI of our cloud, the next step was to give access of the cloud to the user.

The personal cloud can be accessed either wired or wirelessly.

In order to do so, the very first step is to give our Raspberry Pi a static IP address. We can assign it by changing the cmdline.txt file in the boot folder of Raspbian OS.

To provide wired access, connect Raspberry Pi with a switch and provide access to personal cloud via LAN cables.

To provide wireless access, we have to configure the wireless router and then connect it with Raspberry pi via LAN cable. After that, we can connect our device with Wi-Fi and can get access to our cloud.

Experimental Results

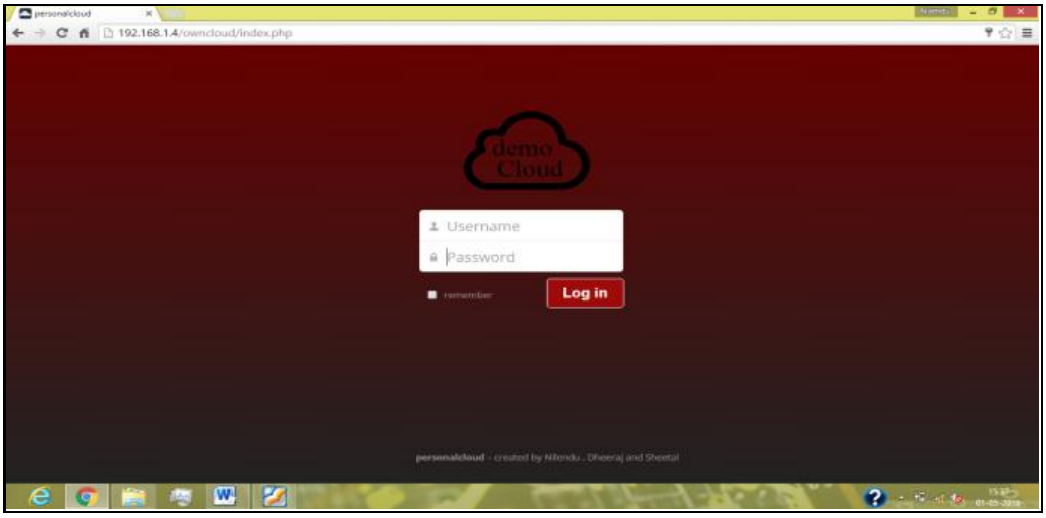

Fig 1: Client side login page

Above figure shows the login page of personal cloud server.

Figure 2 shows the snippet of admin login page of the personal cloud server.

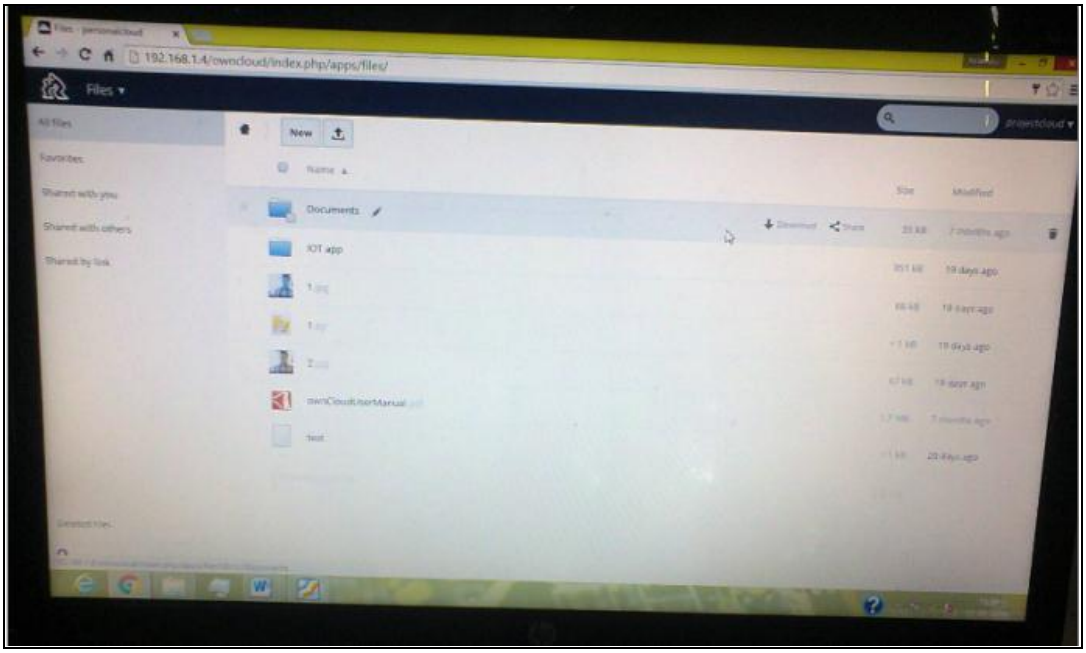

Fig 2: Admin Login in personal Cloud on client side

Logout page of the personal cloud server is shown below

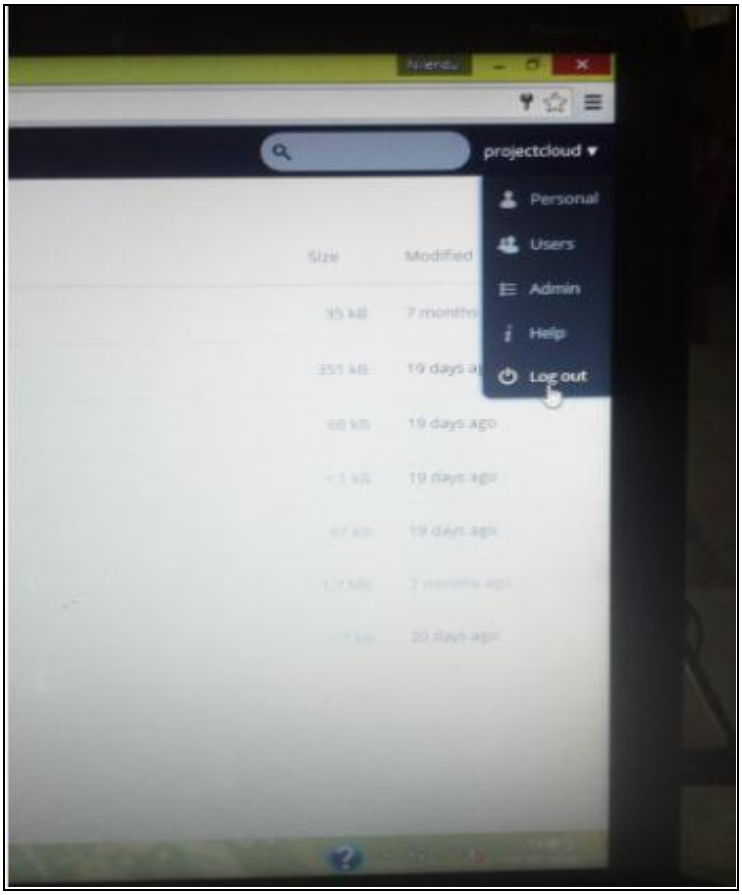

Fig 3: Log Out page of personal cloud

An IoT application is shown in the Figure 4and its web interface is shown in Figure 5.

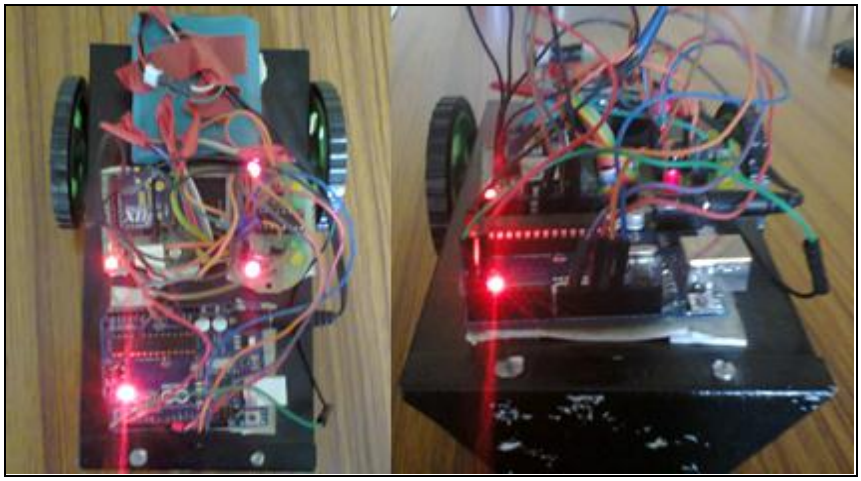

Fig 4: IoT Controlled Bot

Fig 5: Web Interface to control Car

Research Implications

Our proposed work of Personal Cloud Server offers diverse advantages like high speed data transfer, secure data location and accessibility, no third party control, privacy, portability of the cloud server and the most importantly it covers the cloud security in a broad aspect. Security threats like Data security, network security and communication security can be allayed to a large extent with the help of Personal Cloud Server. Also we have demonstrated how this personal cloud can be used as a platform for developing an IoT application and android applications.

Limitations

The most astounding thing about security is that it can always be breached. The proposed product is at early stage of development and still many things need to be incorporated to launch it as a finished product not only for personal use but for different organizations even at the large stage.

Work has to be done to make this product scalable, more flexible, and more user-friendly keeping the hardware and cost as low as possible at the same time. Also when we access the personal cloud over the internet some more security measures are needed, such as Wi-Fi security, network security. This work addresses the basic needs for providing improved security mechanisms in cloud, guiding forthcoming researches in the security area.

Conclusion & Future Scope

The field of Cloud Computing is still emerging in the areas of research and application and still many leaves are required to be unfolded to make it nearly completely secured platform. In this paper, we have outlined the cloud technology, its models and examples, advantages and disadvantages. The biggest challenge faced in cloud computing is of security and privacy. Using the Personal Cloud Server as proposed in this paper, one can ensure portability, data privacy, data security, authorized access control, secure data location and data availability. We have also provided a user friendly application using android OS for wirelessly accessing the cloud from anywhere over the network. Also, we have used the Personal Cloud Server as a development platform for developing an IoT application.

As evolution is a continuous process, a lot is needed to be enhanced and explored.

References

1. Cloud Computing: Issues and Challenges, Tharam Dillon, Chen Wu and Elizabeth Chang, 2010 24th IEEE

International Conference on Advanced Information Networking and Applications.
2. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing, Cong Wang, Qian Wang, Kui Ren and Wenjing Lou. IEEE Inficom Proceedings, 2010.
3. The Security of Cloud Computing System enabled by Trusted Computing Technology, Zhidong Shen and Qiang Tong, 2010 2nd International Conference on Signal Processing Systems (ICSPS).
4. Research on Cloud Computing Security Threats using Data Transmission, Raj Kumar, International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE). January 2015; 5(1),
5. A survey on top security threats in cloud computing, Muhammad Kazim and Shao Ying Zhu, International Journal of Advanced Computer Science and Applications, 2015; 6(3).