IJCTA, 9(37) 2016, pp. 637-642
© International Science Press

Secure Utilization of Resources VIA Internet Between Personal Devices

Andrew Moses* **and G. Emmanuel Johnson****

Abstract: Internet has been used to share data for a long period of time. The paper proposes a system that connects all personal devices of a user as one in a more secured and simple way. This makes all the resources and utility accessible from any device. This eliminates the need of separate dedicated servers. The system uses the resources that are available and ensure that it's used by all the devices. In real time we could process a data using the physical resource and use it using the user's handheld devices. So the user need not worry about utility and resources at any time. For example the user could make his presentation using his handheld device, but the processing and creation is actually done in his home PC. This is very much cost effective and can be used whenever needed. It is made secure via secure shell scripting so that the resources are used by the user alone and no one else. We use an application that helps us to access the resource of other device. It also eliminates the need for cloud and other services. It is fast and cheap.

Keywords: Secure shell scripting (SSH).

1. INTRODUCTION

The internet is a globally connected network system that uses some standard protocols to link several billion devices around the globe. From its early existence, in few years it has become very powerful and has changed the lifestyle of people. It made communication between people easier and changed the business industry totally and took it to the next level. Internet is growing day by day. The most notable evolution of internet [1] is mobile technologies, internet of things (IOT) and social web. Social web has made communication a lot simpler and ensure people are connected together. The internet of things [2] is booming recently giving way to home automation and other things that make life easier. The mobile technology ensured that people are connected to the internet on the go. Hence people can share data from anywhere at any time. The other notable evolution of internet is cloud computing which provides services to people. These services are provided by agents and vendors; hence the services are not reliable and are prone to risks [3] like loss of data, security issues and the need to be dependent. Cloud computing is a complex structure with dedicated servers and several other resources which makes it possible only for the agents and vendors to set up and maintain. It is difficult for an individual to share all his resources across all the devices without relying on an agent or a vendor.

Since the number of personal devices has increased and internet is available worldwide, users have been increasing day to day. Users demand the need of accessing all their personal devices and home network. Certain services are introduced to meet the demands. Specialized middleware are used to have a secure home access and control over the devices [4].

This paper is organized into four major sections. The second section involves with the literature work, the third section involves how the system is structured and how it works and the fourth section involves how it is implemented in real time and the fifth section involves how the proposed system can be further improved in the future. Later the paper is concluded in the sixth section and the necessary references are listed below.

* Department of Computer Science and Engineering, SRM University, Kattankulathur, Kancheepuram, Tamil Nadu, Chennai 603203, India. *9445537210, Email: andrew2moses@gmail.com*

** Department of Computer Science and Engineering, SRR Engineering College, (Affiliated to Anna University, Chennai), Old Mamallapuram Road, I.T High Way, Padur, Chennai, Tamil Nadu 603103, India. *9500174674, Email: bobims.16@gmail.com*

2. RELATED WORK

The present home DNS or remote access can be used to access a particular home service and the current setup uses a gateway device like a modem to get access from the internet where the connection to the home router is dynamic. But this can be overcome by using dynamic DNS or NO-IP. Other methods to connect internal device from a router is using port forwarding techniques, VPN, HTTP proxy. Port forwarding supports TCP or UDP protocols and VPN uses IPv6 where every device has a unique address and help in connecting to a remote client as if they are directly connected. In all these use cases special software or additional configurations has to be installed. Moreover the quality of the system is not analyzed properly [5]. But this paper proposes a framework where these problems can be addressed effectively.

On focusing security issues, a security framework is used between shared devices and this framework addresses the security issues on four categories. They are time dependent devices, privileges difference, capacity limits and device process interrelationship. To grant controlled access several models have been used such as DAC, MAC and RBAC. Among these RBAC are found to be better. So a better approach is done by using RBAC along with XML technology which focuses on the attributes without considering protected objects and accessing policies [6]. Even though this approach seems to be better in security aspects, the overall model is complex and depends on Xport project which comes under grid technology. This technology is immature and is far from reality.

Another issue is energy consumption in mobile devices while accessing remote resources where this is not the case in PCs and laptops because they have a stable power supply. This issue needs to be given more importance because many users use mobiles and tablets instead of PCs. The computing power of desktops can be brought into hand held devices which is a great advantage. Applications like Thinkair and MAUI helps to automate the whole process and focuses on devices based on energy consumption [7]. Among many different remote desktop protocols, there are three prominent protocols namely VNC, RDP and TeamViewer were chosen.

A study on these three protocols was done to measure the energy consumption that these protocols used to access remote resources from devices.

From the study, it can be inferred that all the three protocols had similar energy consumption results. This is because all these protocols had a similar approach. This paper proposes a system which minimizes the use of resources while accessing remote device which gives promising symptoms of better energy consumption.

The UPnP based and Cloud based connections are better than the Bluetooth and Infrared because they required the devices to be within a short distance. This encouraged the advancements in remote accessing developments.

For secure data communication SSH, SCP, SFTP and other transfer protocols are used traditionally. SCP and SFTP are applications of SSH and are used to replace old RCP command and FTP respectively. This is because all the telnet traffic is unencrypted and anyone can intercept even the username and password. The secure copy or SCP doesn't have file management capability and when requested by a client, the server feeds the client with all its directories and sub directories, thus causing server driven download and making the protocol a security risk if the server is compromised. SFTP requires the client to install keys on the SFTP server. SSH uses keys like PGP for security and is quite effective for communication. The Secure Shell is recommended software package for connecting remote computes. All the SSH traffic is encrypted (as seen on Figure 1) from the moment the user is prompted for the username and password till the moment they exit or logout the connection. But SSH is mostly used by web developers to access their files remotely and work with it.

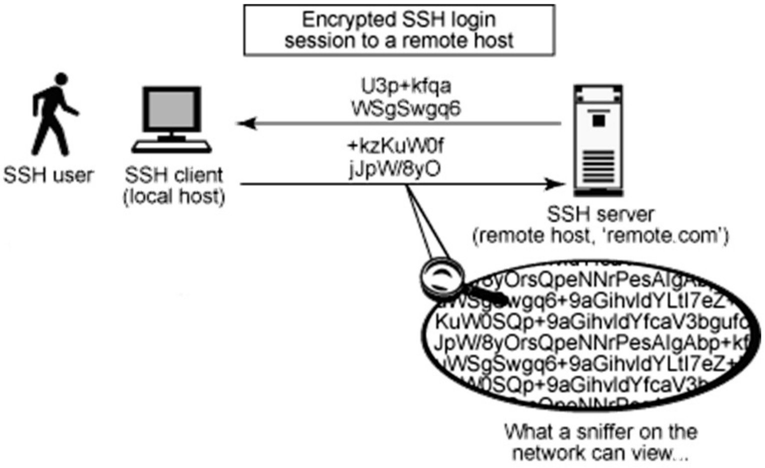
Encrypted SSH login session to a remote host
U3p+kfqa
WSgSwgq6
+kzKuW0f
jJpW/8yO
SSH user
SSH client (local host)
SSH server (remote host, 'remote.com')
What a sniffer on the network can view...

Figure 1: SSH Connection

3. PROPOSED SYSTEM

The system proposed in this paper uses the current technologies like internet and SSH to be used in a more effective and useful manner. The system proposed aims in connecting all the personal devices like PC, laptops and smart phones of a user to be used as a single resource. This makes the resource and utility of one device to be accessible from another device of the user. This system is used as a distributed file system and can be used to access the processor function which helps in scaling resources horizontally. We integrate the hardware and software resources of each device into one. For example, if a laptop with a webcam doesn't have video calling software and the user's PC has software for that purpose, using this system the user can access the software from the laptop and do video calling in real time. This combines the hardware (webcam) and the software behaving like a single machine. This helps in reducing the cost of buying resources for each and every personal device. The system is made secure by Secure Shell (SSH) which encrypts all the transmission among the user's devices. The resources can only used by the particular user and not by others. This eliminates the use of dedicated servers as seen in cloud.

A. Design and Architecture of the Proposed Framework

The system proposed interconnects all the personnel devices through the internet. This is done via secure SSH tunnelling. For this to work all the personnel devices has to be UNIX platform based system. This is because we could access the shell directly via the SSH. However this can also be done on Windows based platform using some free software like putty. But this cannot be done in windows based mobile phones because it doesn't allow root access. The user from one device logs into another device which is in remote location by providing the username and password. The RSA can be used for passwordless access to the system by the user. Once this is done the user can execute shell commands on the remote machine. By this we use the resources of the remote machine. All that the system does is taps the remote system and gets the required data in the form of files, audio or video and deliver it to the system accessing it. Hence we could access any software or hardware of the remove machine through shell commands.

The Figure 3 shows the overall architecture and design of the proposed system. It is seen that all the personnel devices are connected with each other via internet. One major problem in connecting to the remote device is dynamic IP address. The user cannot always be aware of the machines public IP address. For this we can use free services like noip.com which will assign a domain to the devices' IP and update the IP when it changes over time. By this we ensure that the user can connect to the device anytime easily without any problem.

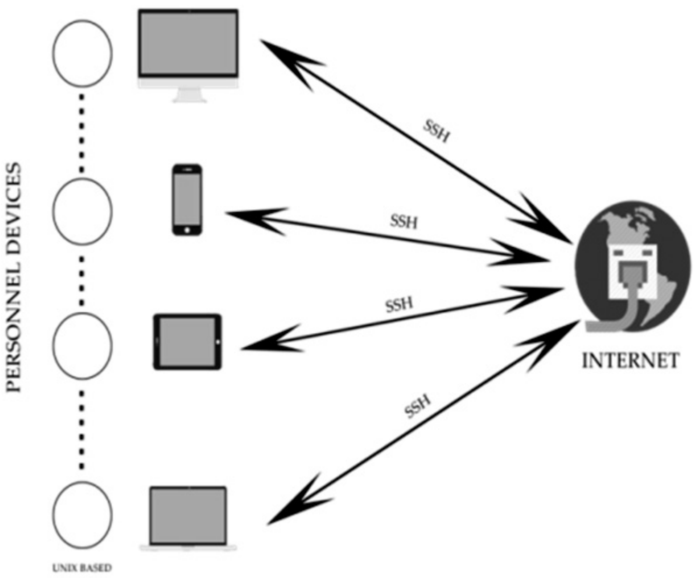

Figure 2: Architecture of the proposed system

B. Technology Used

The Figure 3 shows the flow chart of the proposed system. At first the user gives request from one device to the remote device which is to be used. The request is given via SSH command with the remote devices' domain name. Now the device searches for the IP address of the requested domain name. This is done using noip.com which provides free service in updating the IP address and assigning a domain name to it. Now the SSH requests the remote device and creates an encrypted tunnel through which communication and data transfer takes place. This makes sure that no one can interrupt or steal the transmitted data. The RSA is used for password less access and is authenticated by the pub keys which consist of two keys, one which is secure and the other one is public. When this is successful Shell access is granted to the requested device. Now the user can execute shell commands on the remote system and use its resources. The technologies used in this system are exists, but is used here for another purpose. SSH is traditionally used mostly by web developers to access their files from the server and work with it. Here we use SSH for a more powerful reason thus making the system much secure than without it.

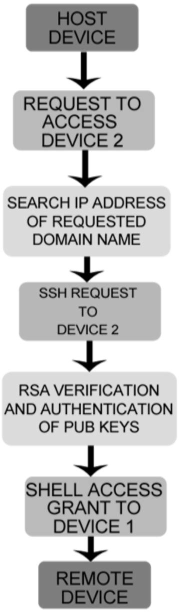
HOST DEVICE
REQUEST TO ACCESS DEVICE 2
SEARCH IP ADDRESS OF REQUESTED DOMAIN NAME
SSH REQUEST TO DEVICE 2
RSA VERIFICATION AND AUTHENTICATION OF PUB KEYS
SHELL ACCESS GRANT TO DEVICE 1
REMOTE DEVICE

Figure 3: Flow chart of the system

4. IMPLEMENTATION OF THE SYSTEM

The algorithm of the system, used for its implementation is very simple and straight forward. It is as follows,

```
Begin
    Get the IP address of the device to which the connection is to be established
    Using SSH, login into the shell via command line
    If login is successful
    Begin
        Start the required application from the shell
        While TRUE
        Begin
            The output from the remote device is converted into transferable data.
            Small packets of data are sent to the host via SCP command.
            As the data packets are received it is appended to respective files.
            The received data are used by the output devices of the host dynamically
        If connection needs to be ended
            Break
    The receive data from the device is used by the host using the required application
End
```

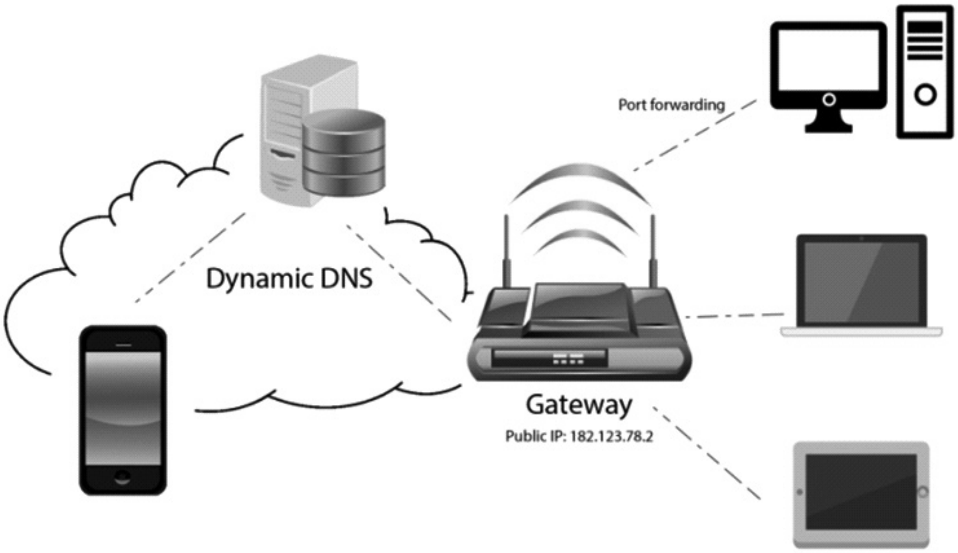

Figure 4: Overview of accessing resources using a remote client

5. FURTHER IMPROVEMENTS AND APPLICATIONS

The system cannot connect to windows based mobiles since there is no root access. So in future overcoming this could interconnect a wide range of personnel devices. Even devices like smart TV, streaming devices, game stations (PS4 and xbox one) can be added to this list which could enable the user to control his personnel device from anywhere. The major limitation of this system is a stable internet connection. But many countries now have a very powerful internet available for the public and can be used for the benefit of this system. We can also extend its use to business levels for more efficient and cheaper way of data access.

6. CONCLUSION

The system proposed can serve a great use for the people who travel lot and have many personnel devices. It is very simple and easy to setup. It doesn't require any additional cost and is very much reliable. The system can be improved a lot by connecting other devices like smart TV, game stations like PS4 and much more.

References

1. Dan Yang ; CompleX Lab., Univ. of Electron. Sci. & Technol. of China, Chengdu, China ; Zhihai Rong; "*Evolution of the Internet at the autonomous system level*", Control Conference (CCC), 2015 34th Chinese, pp. 1313-1317.
2. Ganz, F. ; Centre for Commun. Syst. Res., Univ. of Surrey, Guildford, UK; Puschmann, D.; Barnaghi, P.; Carrez, F.; "*A Practical Evaluation of Information Processing and Abstraction Techniques for the Internet of Things*", Internet of Things Journal, IEEE , Volume: 2 , Issue: 4 , 2014, pp. 340 – 354.
3. Kwang Mong Sim ; Sch. of Comput., Univ. of Kent, Chatham, UK; "*Agent-Based Cloud Computing*", Services Computing, IEEE Transactions on Volume: 5 , Issue: 4 , 2012, pp. 564 – 577.
4. Marin, A.; Mueller, W. ; Schaefer, R. ; Almenarez, F. ; Diaz, D. ; Zigler, M.; "*Middleware for Secure Home Access and Control*", Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on March 2007, pp. 486 – 494.
5. P. Belimpasakis, A. Saaranen and R. Walsh; "*Home DNS: Experiences with Seamless Remote Access to Home Services*", World of Wireless, Mobile and Multimedia Networks, IEEE International symposium 2007, pp. 1-8.
6. Li-Guohui, Luo-Tiejian, Song-Jinliang, Xu-Yanxiang; "*A Security Model for Online Accessing to Shared Devices*", Networking, Sensing and Control, 2006. ICNSC '06. Proceedings of the 2006 IEEE International Conference on 2006, pp. 143 – 149.
7. Youming Lin and Mario Di Francesco; "*Energy Consumption of Remote Desktop Access on Mobile Devices: An Experimental Study*", Cloud Networking (CLOUDNET), 2012 IEEE 1st International Conference on 2012, pp. 105 – 110.