An Investigation of Using Privilege Level System to Restrict Employers for Using Unpermitted Website

Roza Hikmat Hama Aziz *roza.hamaaziz@univsul.edu.iq*
Computer Science Department
Faculty of Physical & Basic Education
Sulaimani University
Kurdistan Region-Iraq

Miran Hikmat Mohammed Baban *miran.mohammed@univsul.edu.iq*
Computer Science Department
Faculty of Science
Sulaimani University
Kurdistan Region-Iraq

Ako Muhammad Abdullah *ako.abdullah@univsul.edu.iq*
Computer Science Department
Faculty of Physical & Basic Education
Sulaimani University
Kurdistan Region-Iraq

Abstract

This paper provides the security level for employees in the organization that prevents them to use or to browse some website that are not allowed to be seen during work time. However, there are many ready software tools have available which do the same task, but we will try finding a new algorithm to investigate the better solution for this research question. The main reason of our research is to provide an open source software that can be easily manipulated by providers rather than ready software. For example, tools that cannot be updated by the organization administrator (none open source software).

Keywords: Personal Computer, Encryption, Decryption, Web Links, Privilege, Semi-Restricted, Smart Phones, User Interface.

1. INTRODUCTION

One of the today issues lots of offices have lots of employees working on the sensitive part of the system that related to the organization. In some cases, employees may do not obey the rules of the organization that they worked for it. For example, they may open some website that is not permitted by the organization, and this will affect the system of organization because of viruses and hackers.

In addition, the members who are staffed by the organization company may be busy and lost their times with opening useless website that are denied by company manager. There are many websites that are not allowed freely to watch (games website, Facebook, Twitter, YouTube and some other website). Also, these types of web pages will slow network in the organization.

In order to solve this phenomenon is to restrict every user to the group with disallow website. This solution can be done by implementing MAC address and IP address restriction system on each computer office building and also implementing the hierarchy of privilege level computer users.

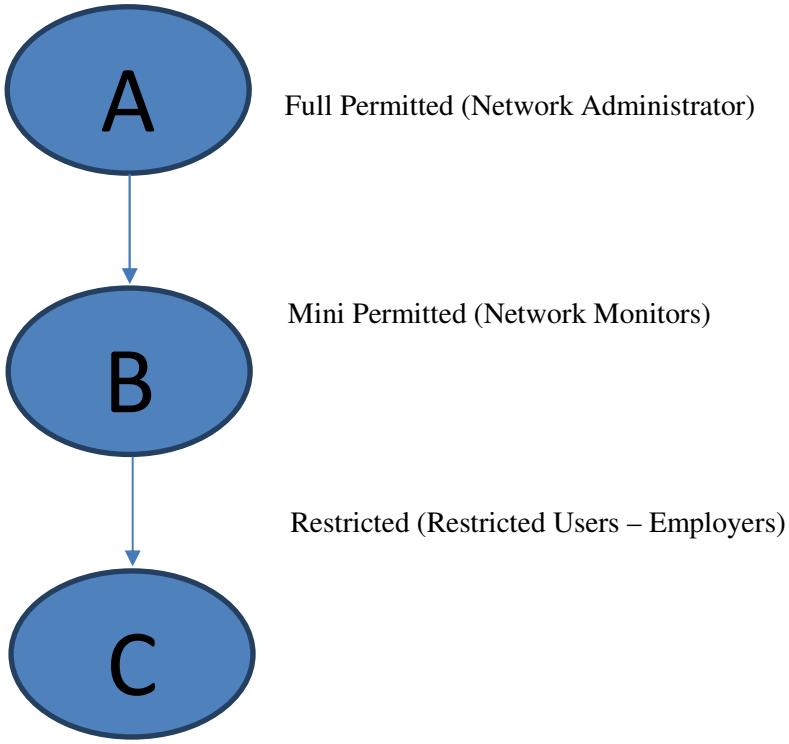

FIGURE 1.1: Privilege System Levels.

1. Level A means the administrator of the networks in the organization which will administrate all the actions that will be done by the employers and monitoring staff.
2. Level B (Mini Permitted) works by monitoring people in the organization and blocking every user who tries to open unpermitted websites.
3. Level C (Normal Users) who are members of the organization (employee's staff).

This paper will try to discuss the two ways of given privilege for the users in the company:

1. Method (1): permission by IP Address
2. Method (2): permission by MAC Address

In method one each client has their IP address that restricted some websites that mean the level C will be permitted IP protocol.

While, Second method will work on level two (Monitor Staff) will give an Authorization permission to use the system using MAC address verification.

2. LITERATURE REVIEW

A. Web Security

Public awareness of the need for safety in computing systems is growing as critical services are becoming increasingly dependent on interconnected computing systems. National infrastructure components such as the electric power, telecommunication and transportation systems can no longer function without networks of computers [6]. The World Wide Web has advertised and increased public concern for security. Safety is the primary concern of businesses that want to use the Internet for commerce and maintaining business relationships [5].

B. Security Level

Level of safety is an important issue for people these days because it will hide sensitive data from unpermitted users. Thus, it is very relevant that each organization has their security level between

system and users. For instance, the administrator of the organization may divide the concept of safety into some levels [4].

C. Administrators Roles

By Providing a security environment, there will be an important Ideal to have a proper administrative who can manage all the data related to the organization that the employees work there. This problem happens because not all of the employees have the same attitude towards using internet and computer [1].

In addition, employees may use their mobile phone or smartphone for networking and browsing. Also, there must be the same restriction on those mobile phones through the organization networking system by implementing the same idea of computer restrictions [2].

D. Networking Database

This practical work comprises database, networking, programming paradigms and security algorithms. In addition, we will provide a backend server to store all the information related to our work. We use database to store information about user action (log file), and networking is our primary essential media connection that will connect all the devices to the server through wireless networking system. In addition, the programming subject is for creating a security algorithm that will work by dividing the security privilege for users into three sub-levels. Full restricted (Level A), semi-restricted (Level B) and unrestricted (Level C) [9].

E. Media Access Control (MAC) Address

One of the another layers in the networking system, it is called layer two also in the networking concepts it named Data Link Layer that is the layer that come after physical layer. Networking system needs all these layers and especially MAC address layer that is the way distinguish between the computers in the large LAN networking system. Also, the privilege of the system to restrict the users can be set by MAC address [8].

F. Operating System Security Mechanism

The increased awareness of the need for security has resulted in an increase of efforts to add security to computing environments. However, these efforts suffer from the flawed assumption that security can adequately be provided in the application space without certain security features in the operating system. [7]. The computer industry has not accepted the critical role of the operating system to security, as evidenced by the inadequacies of the basic protection mechanisms provided by current mainstream operating systems [17].

G. Cloud Computing

It is another way to make or to provide a remarkable connection system among different devices including IOS such as iPhone, IMac, IPod IPad, and Android. Besides those devices other mobile communication devices can connect to computer devices to exchange various kind of data for instance images, voices, text, and video. Nowadays, it is very common that employees use smartphones regularly, and it became a daily habit. Thus, employees will be busier with using their mobiles rather than their obliged job in their office and organization [10]. We have three types of cloud delivery model

1) Software as a Service (SaaS)

There is some software that provide and easy way to access the network of clouding system which help users to communicate with each other to share data. This software is working based on web interfaces that help users to investigate the way to becoming a member of clouding system [12].

2) Platform as a Service (PaaS)

This cloud software has been manipulated to work on some platform for example Linux, Windows, and Mac. In this way, the manufacturers of the cloud software used some programming languages in order to provide an environment platform that can load the clouding system

software. Thus, each operating system platform has their cloud software system will be vary from the other OS [12].

3) Infrastructure as a Service (IaaS)

In addition to Platform as Service (PaaS) and Software as Service (SaaS), there is another property of clouding system model that is Infrastructure as Service (IaaS). This platform works for storing all information that have been used by the system users of the clouding system. In addition, this can work as an investigation on users' activity in the system, which means that will look into log files [12].

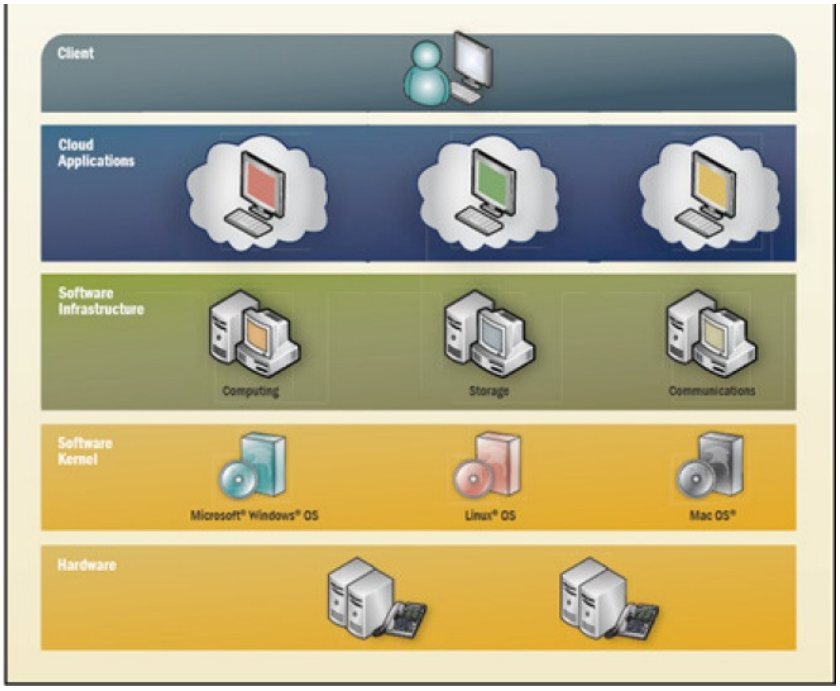

FIGURE 1.2: Cloud Computing Modeling.

H. Cloud Service Deployment and Consumption Models

Regardless of the delivery model utilized (SaaS, PaaS, IaaS) there are four primary ways in which cloud services are deployed. Cloud integrators can play a vital role in determining the right cloud path for a particular organization.

1) Public cloud

Public clouds are provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment.

In addition all the benefits and functionality of elasticity and the accountability/utility model of cloud.

The physical infrastructure is owned by and managed by the designated service provider and located within the supplier's data centers (off-premises).

All customers share the same infrastructure pool with limited configuration, security protections, and availability variances. One of the advantages of a public cloud is that they may be larger than an enterprise cloud, and hence they provide the ability to scale seamlessly on demand [11].

2) Private cloud

Private clouds are provided by an organization or their designated services and offer a single-tenant (dedicated) operating environment with all the benefits and functionality of elasticity and accountability/utility model of cloud. The private clouds aim to address concerns on data security and offer greater control, which is typically lacking in a public cloud. There are two variants of private clouds: (i) on-premise private clouds and (II) externally hosted private clouds. The on-premise private clouds, also known as internal clouds are hosted within one's data center. This model provides a more standardized process and protection but is limited to aspects of size and scalability. IT departments would also need to incur the capital and operational costs for the physical resources. Thus, it is best suited for applications that require complete control and configure the ability of the infrastructure and security. As the name implies, the externally hosted private clouds are hosted externally with a cloud provider in which the provider [13].

3) Hybrid cloud

Hybrid clouds are a combination of public and private cloud offerings that allow for transitive information and possibly application compatibility and portability across disparate cloud service. This cloud will offer and provide utilizing standard or proprietary methodologies regardless of ownership or location. With a hybrid cloud, service providers can utilize third-party cloud suppliers in a full or partial manner, by that increasing the flexibility of computing. The hybrid cloud model is capable of providing on-demand, externally provisioned scale. The ability to augment a private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload [15].

4) Managed cloud

Managed clouds are provided by a designated service provider and may offer either a single-tenant (dedicated) or multi-tenant (shared) operating environment. With all the benefits and functionality of elasticity and the accountability/utility model of cloud. The physical infrastructure is owned by and/or physically located in the organizations' data centers with an extension of management and security control planes controlled by the designated service provider [16].

3. SYSTEM REQUIREMENTS

A. Software

- Programming Language: Net C#
- Database: MySQL
- Operating System: Linux (UBUTNU) and Windows Server

B. Hardware

- Desktop
- Laptop: Intel (R) Core (TM) 2 Duo CPU T6600 @ 2.20GHz, Memory RAM 2GB, System Type: 32 bit Operating System.
- Server
- Switch
- Cables
- RJ 45
- Wireless Router

4. SYSTEM TESTING

This system has been tested on a local network between many computers connected to a server that services all the clients. We have used the both techniques of the network connections wired network and wireless network. It has been noticed the customers who have been restricted to

some websites for instance YouTube; it cannot be open. This due to the particular IP address blocked to use YouTube.

On the other hand, the monitor's part cannot access all the client only the group that permitted by the administrator for example computer namely (Comp1, Comp2, and Comp3) cannot be controlled.

5. RESULTS AND DISCUSSION

In our work, we have done some setups of security levels, and we tried to block accessing some website under the IP address for the clients. In this way, we can prove that the network (LAN) in the organization can be under control by the monitoring system staff. The following we show the steps of banning IP address for accessing some website:

A. First Step Start with Login Form

In this form administrator and monitor, staff should use their username and password to access the system. This step uses as a security measure to prevent accessing by other people out of the system. As shown in fig 1.1.

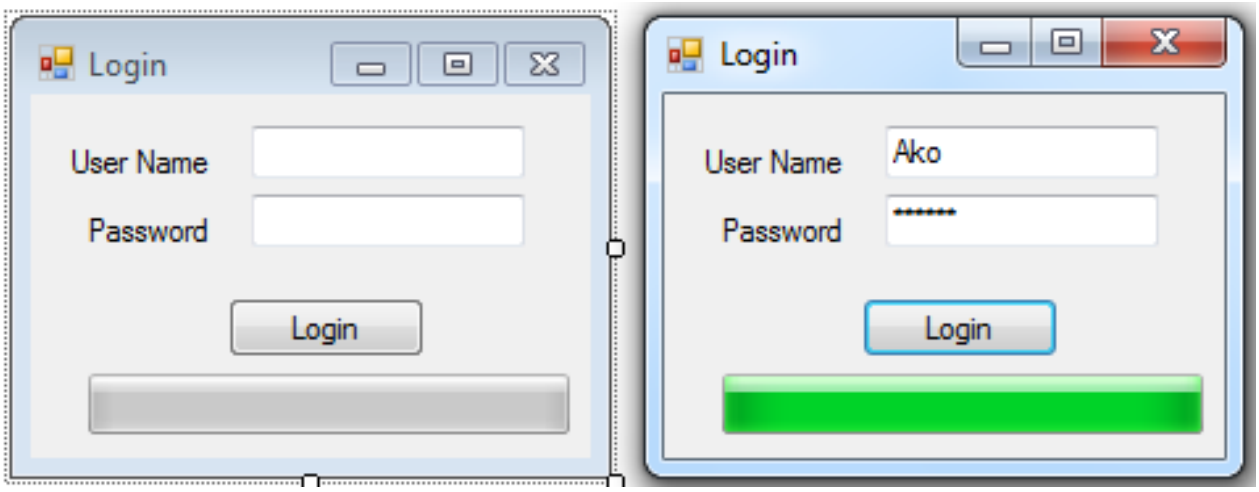

FIGURE 1.3: Login Form.

B. Second Step Blocking Websites and IP Address

In this step monitoring staff will get the form of the blocking website after the login successfully. As the screen clear from the following figure.

FIGURE 1.4: Blocking Website Form.

C. Third Step Filling Form

In this step, the entire field should fill completely. There is two text box one for inserting the IP address of the client that we want to band the accessing website that we will enter in the second text box as is evident in the following figure. After that, the button that name "**Block Above Website,"** this button will block the client with specified IP address to access the website "YouTube." The other buttons one for unblock website and the last one for unblock all internet site.

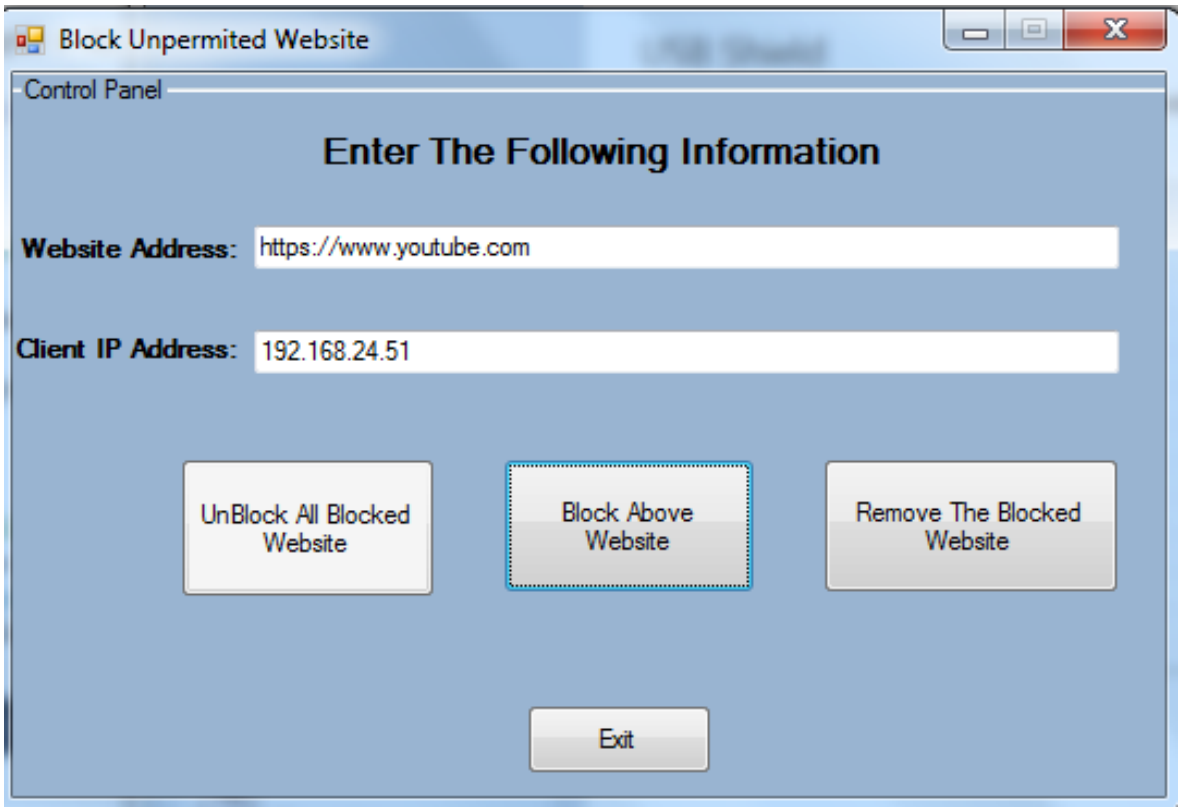

FIGURE 1.4: Blocking YouTube Website.

D. Fourth Step Saving the Hosts File

After the monitor worked on blocking a specific website for a particular client IP Address, the action will be stored in the file called hosts. This file is located in drive C: and especially in ("C: \Windows\System32\drivers\etc") as it is evident in the following figure.

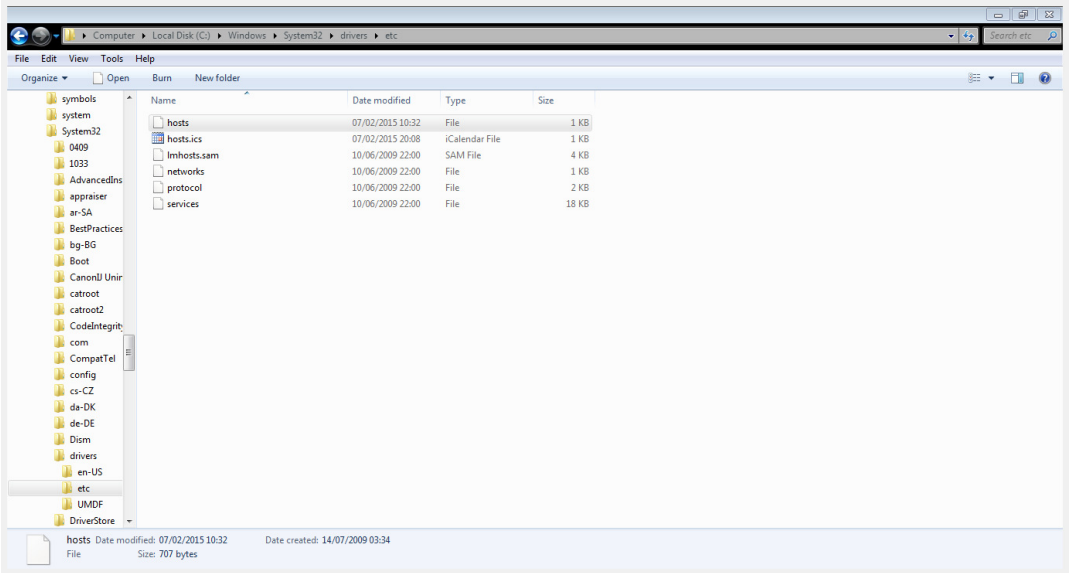

FIGURE 1.5: Hosts file (Exact Location for Hosts File).

The content of this file, consist of blocked website and client IP address, as it can be seen, that the specified IP address located on the left side of the file for instance, IP address "**192.168.24.51**". Also, it can be noticed that the web address that required to be banned is located on the right side of the document, for example, "**www.youtube.com**".

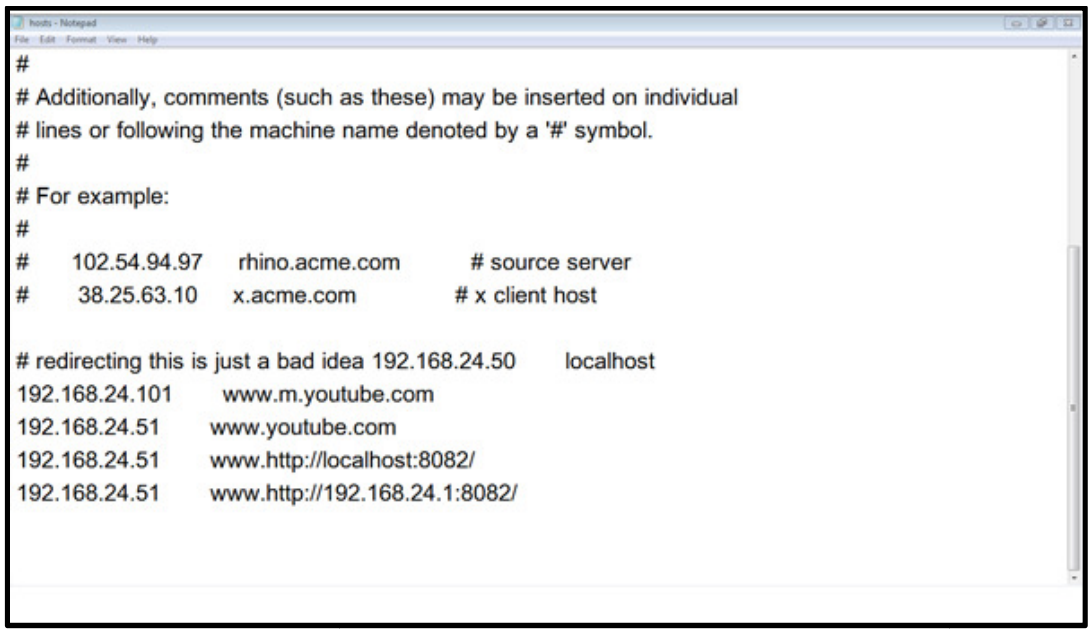

FIGURE 1.6: Hosts File (List of Blocked Website).

E. Blocking Websites and IP Address Feedback

After inserting the required data in the text box that specified in the form for example text field named "Website Address" and the second one is called IP address. We will get a feedback message box tell us our blocking process has been done successfully or unsuccessfully. As shown in fig (1.7).

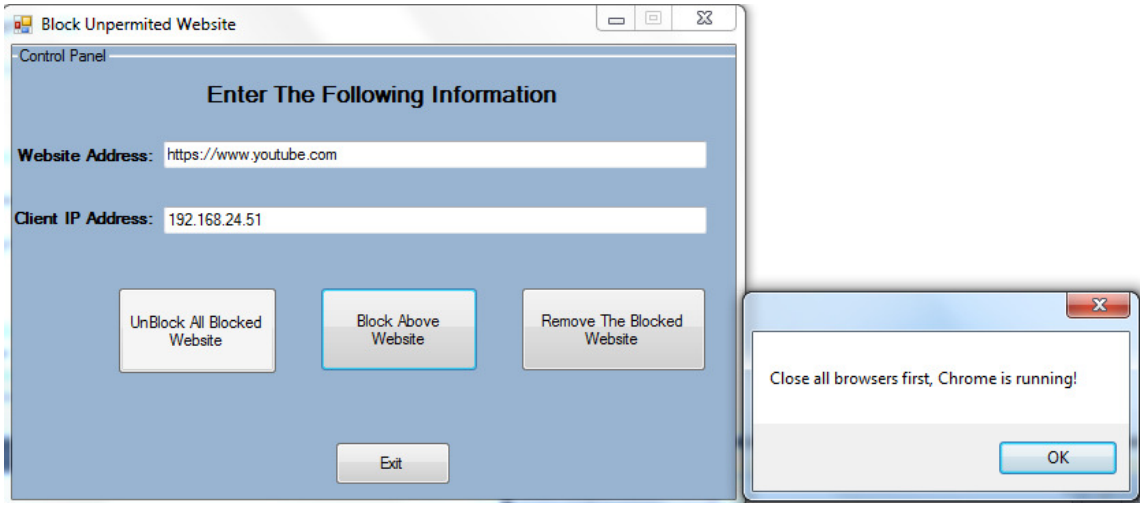

FIGURE 1.7: Successfully Login Website.

F. Unsuccessful Website Output

After the website is blocked by the monitoring staff, for instance “www.youtube.com." It can be seen from the client side that specified IP address cannot open the link that is blocked following figure is an example of blocking result.

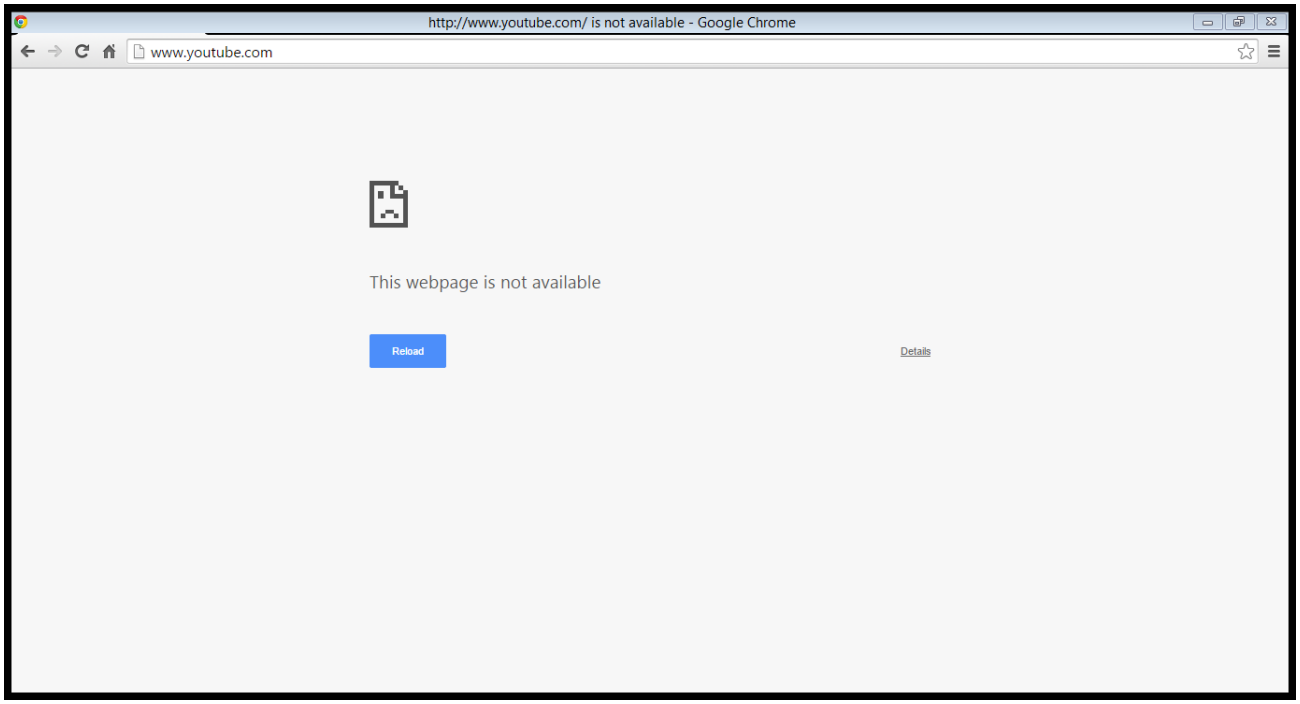

FIGURE 1.8: Blocking Website Output.

6. CONCLUSIONS AND FUTURE WORK

After proposing a new idea for blocking web pages that are not permitted to be access in public organizations by their staff, we come to account that we have a possibility to give a role of blocking website to monitoring staff that monitors the group network access that can block any website based on the client IP address. From this way, we control the entire client over the network and limit their capability to access the public website, for example, YouTube. Additionally, this new system will return lots of time to their staff to work within the organization instead of losing time with some website that is not permitted.

On the other hand, this system is tested on mobile devices as well. For instance, (iPad, Android (Samsung Galaxy 4) and IOS (iPhone), the same action can be performed on them, and this can be done through Connected IP address. This will less the chance to use mobiles and page surfing during workload times.

Our plan for the future work, we will expand our to a the bigger area of network comprising the control of two organizations at the same time. In addition, we activate the role of administrator level to grant and revoke permissions from monitors' staff, based on IP Address and their level of system Accessibility. In addition, we create another part for blocking which though mac address. Client will be banned to access some website through using their computer MAC Address.

7. ACKNOWLEDGMENT

We would like to thank our university (University of Sulaimaniyah), for all help and facilities that gave us while proposing this research. Also, we would like to thank everyone who helps us.

8. REFERENCES

[1] Loscocco, P., Smalley, S., Muckelbauer, P., Taylor, R., Turner, S. and Farrell, J. (1998). The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments. Vol. 10, pp.303-314.

[2] Xing, L., Pan, X., Wang, R., Yuan, K. and Wang, X. (n.d.). (2012). Upgrading Your Android, Elevating My Malware: Privilege Escalation Through Mobile OS Updating, pp. 1-16.

[3] Hudson, J. and Bruckman, A. (2005). Using empirical data to reason about internet research ethics. pp.287--306.

[4] ERIC, M. and Goetz, E. (2007). Embedding information security into the organization.

[5] S. Garfinkel. Web Security and Commerce. O'Reilly & Associates, Cambridge, 1997.

[6] President's Commission On Critical Infrastructure Protection. Research and Development Recommendations for Protecting and Assuring Critical National Infrastructures, September 1997.

[7] B. Blakley. The Emperor's Old Armor. Proceedings of the New Security Paradigms Workshop, 1996.

[8] Abdullah, A., Baban, M. and Hama Aziz, R. (2014). A New Approaches to Improve Server Secuirty by Using Media Access Control Address Verification. A New Approaches to Improve Server Secuirty by Using Media Access Control Address Verification, 15(2), pp.83-87.

[9] NIST, "A Survey of Access Control Models," NIST Privilege (Access) Management Workshop, available at: http://csrc. nist. gov/news-events/privilege-managementworkshop-2009.

[10] Tari, Z. (2014). Security and Privacy in Cloud Computing. IEEE Cloud Computing, 1(1), pp.54-57.

[11] Sill, A. (2014). Setting Cloud Standards in a New World. IEEE Cloud Computing, 1(1), pp.50-53.

[12] Basu, A., Vaidya, J., Kikuchi, H., Dimitrakos, T. and Nair, S. (2012). Privacy preserving collaborative filtering for SaaS enabling PaaS clouds. J Cloud Comput Adv Syst Appl, 1(1), p.8.

[13] Baun, C., Kunze, M., Kurze, T. and Mauch, V. (2011). Private Cloud-Infrastrukturen und Cloud-Plattformen. Informatik-Spektrum, 34(3), pp.242-254.

[14] Tarannum, N. and Ahmed, N. (2013). Efficient and Reliable Hybrid Cloud Architecture for Big Database. IJCCSA, 3(6), pp.17-29.

[15] Martin-Flatin, J. (2014). Challenges in Cloud Management. IEEE Cloud Computing, 1(1), pp.66-70.

[16] Mostarda, Leonardo, and Alfredo Navarra. 'Distributed Intrusion Detection Systems For Enhancing Security In Mobile Wireless Sensor Networks'. International Journal of Distributed Sensor Networks 4.2 (2008): 83-109.