International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech. 5, No. 3 (Sept.-2017)
http://dx-doi.org/10.12785/ijcnt/050304

Design and Implementation of a Mechanism to Secure the Access in Cloud Computing

Adeeb Hamdoon Sulaiman[1], Hilal Al Bayati[2], and Ahmed Bayouni1or[3]

[1] *Department of Management Information Systems, Applied Science University, Manama, Kingdom of Bahrain*
[2]*Department of Computer Science, Applied Science University, Manama, Kingdom of Bahrain*
[3] *Department of Management Information Systems, Applied Science University, Manama, Kingdom of Bahrain*

Received: 03 Jun. 2017, Revised: 17 Aug. 2017, Accepted: 20 Aug. 2017, Published: (01 September 2017)

Abstract: The main goal of this research is to design and implement a secure mechanism to access a cloud service system by using authentication service, virtual private network, and short message service to achieve security. The authentication mechanism would reject unauthorized access attempts by unauthorized users, while the authorized users will be allowed to access the services by receiving an SMS code on his/her mobile that can be used to log on the service. The system was designed, implemented, and tested successfully.

Keywords: Cloud Computing, User authentication, Virtual Private Network, Short Message System SMS, and SSL VPN.

1. INTRODUCTION

Cloud Computing became the prominent technology in recent years and has received a lot of attention from researchers, companies, and nonprofit organizations. All this interest comes because of its potential opportunities and expectations. Cloud Computing provides services in many ways such as software-as-a-service, storage- as -a service and many other services. Security is considered a key issue in cloud computing due to the variety of functions, applications, services, and technologies it provides. One critical issue which represents a high risk challenge and threat is Authentication.

Data is regarded as the most critical asset for any organization, which needs to be securely protected in the cloud from unauthorized access. User authentication is needed to enable the user to access the data and applications stored in the cloud and to make sure that it is available when needed for the authorized user only.

Providers of the cloud must provide authentication mechanism to be accessed by authorized users only. If providers neglect authentication procedures, the threat and risks of cloud system security will be increased and it may be accessed by unauthorized users.

For this research the main problem is to study cloud computing security then to propose an enhanced authentication procedure to securely access the cloud computing environment from different devices.

There are many definitions of Cloud Computing; most of them focus on pay- per- use, availability, scalability, virtualization and internet, and hardware abstraction.

For the purpose of this research cloud computing is defined as "a way to deliver the IT services to the users to provide it when they need them. Most of those services are accessible over the internet and users only control and are charged for what they need"[4].

2. CLOUD COMPUTING SERVCES AND ARCHITECTURE

Cloud computing services architecture is mainly classified into three types of services, and these are:

A. Software-as-a-service (SaaS)

Cloud-based applications for (SaaS) run on remote computers within the cloud, which is owned and

E-mail: Adeeb.hamdoon@asu.edu.bh, hilal.albayati@asu.edu.bh, ahmad.bayouni@gmail.com

operated by others who connect to users' computers via the Internet, usually a web browser. Software-as-a-Service (SaaS) is the highest layer of the cloud service as shown in Figure (1). SaaS is defined as the on demand usage of net-native software which is available via a network (e.g. the Internet) by cloud service providers.

For example, Google's Gmail is a cloud-based SaaS application that replaces traditional email programs that run on your computer such as Outlook.

B. Platform-as-a-service (PaaS)

Platform is a cloud-based environment required to support the complete lifecycle of implementing web based (cloud) applications—without the cost or intricacy of buying, managing, and hosting the H/W and S/W [1]. Platform-as-a-Service (PaaS) is the provision of applications or technical framework platforms without spending time on thinking and working on the underlying necessary hardware, operating system and task specific tools. At the moment, the focus for companies of PaaS is on using this concept when developing and running (web) applications for the cloud. Therefore the whole life cycle of the development of a web application and the appropriate workflow is supported and represented in PaaS.

PaaS is especially useful in any situation where multiple developers will be working on a development project or where other external parties need to interact with the development process.

C. Infrastructure-as-a-service (IaaS)

IaaS provides computing resources including servers, storage spaces and networking on pay-per-use [1].

The concept started under the term Hardware as a Service (HaaS) and was later transformed to Infrastructure-as-a-Service (IaaS) to show the holistic approach for all hardware to run an IT infrastructure as a service.

Each customer has his self-provisioned and elastic virtualized IT infrastructure without consideration of the actual underlying physical IT infrastructure. Standardization of IT infrastructure allows the differentiation of storage and computing services; actually computing services follow storage services.

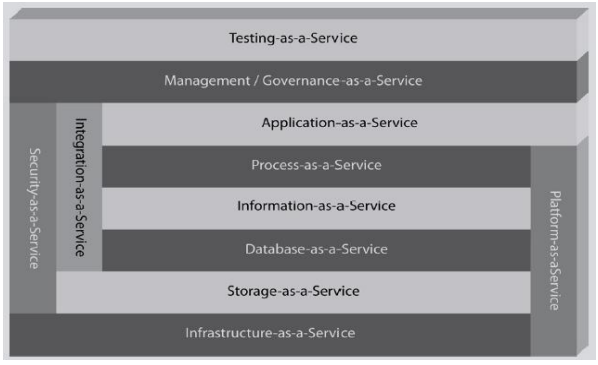

Figure 1. Cloud Computing Services

3. TYPES OF CLOUD STYLING

Clouds are classified either, by location where the cloud is based, or by the service that the cloud offers.

The cloud types based on a cloud location can be described into four types of cloud:

A. Public Clouds

Public clouds are clouds that are available to the public by service providers who support and provide the infrastructure. Generally, the providers create; operate the infrastructure and the services that he offers over the Internet. In this type of cloud, customers do not know where the cloud located physically, and cannot control it. They also share the infrastructure with other customers with limited security protections, availability variances and configuration [5].

B. Private Clouds

The private cloud is a cloud that uses a dedicated infrastructure for each costumer, and it allows them to host applications in their private cloud, and it is used by businesses who are responsible for the security and control of the data and apps. This type of cloud comes out because the public cloud cannot offer full control, so data and applications are not shared with others, but are managed internally, and hosted internally or externally [5].

C. Hybrid Clouds

Hybrid Clouds are a cloud that combines deferent types of clouds to offer the advantages of these clouds' deployment models. The hybrid cloud increases computing due to its flexibility, and provision of public cloud information resources that can be used to manage any unexpected surges in workload [5].

D. Community Clouds

Community clouds is a cloud that is shared between two or more organizations which is governed, managed and secured by all the organizations that use it, or a third party service provider [5].

Community clouds are built and used specifically for a group of organizations that use the same cloud requirements, and the main goal is to work with each other to gain business benefits or objectives.

The main goal of community clouds is to provide the advantage of a public cloud with levels of privacy, security, and policy compliance usually associated with a private cloud.

4. CLOUD SECURITY

Security is one of the biggest information systems challenges to any businesses in any form, whether a small brick-and-mortar business or large online business ventures. The companies always have different security risks which always come from different sources or malicious intent. One security attack could mean the loss of millions dollars for businesses or even close the business down

[6].

The correct implementation of security value is strongly recommended to apply in the cloud computing environment. This is because the data are used, processed and the applications are launched over the internet, exposing it to attack at any time.

Cloud computing security is a unique situation of lasting risks, because its implementation requires millions of dollars in infrastructure and security but it is not exempt from security risks, due to different types of attack.

A. Protecting the Users

Above everything else, any type of online application format, especially cloud computing, should take into consideration the protection of its users [6].

Developers, application programmers, and infrastructure specialists should make sure that information related to the users is not visible and cannot be used or extracted by anyone except the rightful users.

There are two possible ways to make sure that the users are protected in cloud computing; restrictive user access and certifications.

Restrictive user access to cloud computing must start at least from simple username/password; it also must include "CAPTCHA" Completely Automated Public Turing test to tell Computers and Humans Apart.

User time-outs and Internet Protocols IP specific applications provide some, though not enough, of the security standards that should be implemented to secure the users.

The restrictive user access challenge is to limit the access privilege of the end user. To assure the limitation of access to applications or files, every user in the cloud system must be assigned manually with clearance of security.

Certifications; the users must liaise with the security specialists and companies that provide certifications for security about their systems. This can be done through external security checks, by external professional security bodies of cloud computing to certify its security to the end users.

B. Data Security.

As user protection, the data also must be protected against different types of attacks. The software and hardware used in the cloud environment must be scrutinized. In data security, the certification is also an important appliance in this part of cloud security.

The data center must also be protected from different types of natural disasters as weather conditions, fire and even physical attacks that can destroy the data or the hardware.

Among the data security solutions in high risk situations are manual shutdown that is used to prevent further access of the information if the system has been attacked.

Although data control can come from another application, the data can be infiltrated by another application unless it has been shut down immediately [6].

C. Cloud Security Threats [2]

The Cloud Security Alliance (CSA) has classified the security threats of cloud computing into seven types. These are:

I) Abuse and nefarious use of cloud computing:

II) Some of the service providers offer free limited trial services. At the same time, they abuse the use of customer systems, forms, usage models, applications code and private systems if the

customer does not renew the service. Some service providers or vendors especially use attacks that work only on websites targeting the old customer or their competitors. This threat could come from Spam, malicious code authoring, hacking, password cracking, Bot-net, and CAPTCHA. To overcome the abuse and nefarious use of cloud computing threats, we need to implement measures that use strict registration and validation processes, improve anti credit card fraud, and use network traffic monitoring.

III) Insecure interfaces APIs and software access:

Cloud service providers provide many interfaces or APIs "application programming interface" software used by customers to interact and manage their cloud services. APIs must be designed to provide some tasks such as authentication, access control encryption, and activity monitoring, to protect the user and system sides from accidents and security threats. Organizations must develop their own application for the mobile devices (phone and tablets) with strong access authority's methods to access the VPN. APIs, mobile device access authentication (computer, smart phone, tablet, etc.). Due to the fact that all customers of the same service providers use the same APIs and security methods, a customer may be exposed to attack by other customers who have subscribed to the same service provider. Overcoming the Insecure interfaces APIs and software access threat, measures need to be implemented to audit the service provider security measures, use strong authentication and access control systems, and analyze the security of each index/pendent APIs.

IV) Malicious Insiders:

This threat appears when an organization serves many customers under one management domain which leads to a general lack of transparency into providers' processes and procedures. As a provider cannot give customers access to physical assets, or cannot provide the top management with the means to monitor the employees or how to analyse the reports of employees' performance and access log. There is little or no visibility into the hiring standards and practices for customer and employees.

This may create an opportunity for organized crime, for hackers inside or outside to access and harvest confidential data or gain complete control over the cloud services providers [2]. The impact is about a level of access and ability to infiltrate organizations and assets over the providers. It may expose to brand and financial impact and loss of productivity. As an organization using cloud services, humans are an important element to this threat.

These threats may come from hackers, corporate espionage, and state sponsored intrusion. To overcome these threats, measures should be implemented to use strict human resources contracts requirements, transparency in information security management and practices, and the use of security breach notification process.

V) Shared Technology Issues:

Cloud service providers deliver their services by sharing infrastructure to customers. Some of the components of infrastructure such as CPU caches, GPUs, and storage do not offer strong isolation properties for a multi customer cloud architecture.

To solve this issue, providers will need virtualizations hypervisors, who mediate access to share and communicate with the customer operating systems and the physical resources. Still, even after hypervisors its inappropriate levels of resources platform still, even after hypervisors are provided, it might be inappropriate levels of resources platform.

The cloud service providers' strategy should have strong compartmentalization in computing, storage, and network security and monitoring, to ensure that each cloud customer works without any impact on other customers with the operations of the same provider.

Cloud providers must ensure that customers cannot access any other customers' residual data, application and traffic [2].

This threat targets cloud computing providers which uses a shared technology as Disk partitions, CPUs, GPUs, and other elements that are not designed to use in shared technology with strong compartmentalization. It may attack the operations of other cloud customers and impact the service and it may be used to gain unauthorized access to data. [2]. To overcome this threat, measures should be implemented to use security best practices for installation, IT resources monitoring, strong authentication and access control, conduct security

system auditing. IT resources monitoring strong authentication and access control, and conduct security system auditing.

V) Data Loss or Leakage [2]:

There are many threats that can be caused to the data such as deletion or modification without a backup of the original data. The reason for this is using unrecoverable databases, or applications that may be unreliable.

The data threat increases in the cloud; customers must know interactions between risks and challenges of sensitive data and understand the architectural and operational characteristics used by the cloud providers.

Losing data can cause big problems to a business; a loss can impact on employees, partners and customers' trust. Loss may expose cloud customers to competitive and financial implications. The worst thing is that the lost data might be used against the company [2]. To overcome the data loss or leakage threat, measures need to be implemented to use strong APIs access control, in transit data encryption with strong encryption key management processes, and data backup.

VI) Account or Service Hijacking:

This threat can be caused in many ways such as phishing, fraud, and exploitation of software vulnerabilities. Passwords and credentials are reused

Cloud computing services add a new threat. If an attacker tries to access customers' credentials, that means he can eavesdrop on the customers' activities and transactions and data.

The account or service in the service provider's system becomes a new target for the attacker. Hijacking the account and service is always done with stolen credentials and attackers can use it in any critical areas in customer's cloud services. They may use it to compromise the confidentiality and availability of those services. Cloud customers have to be aware of these techniques as a defense in protection strategies. To overcome the account or service hijacking threat, measures need to be implemented to prohibit the sharing of account credentials, using proactive monitoring to detect unauthorized activity, and ensure understanding of cloud computing security policies.

VII) Unknown Risk Profile:

As any technology related to IT, it must ensure the hardware and software ownership and schedule maintenance to make companies focus on business strong points and financial and operational benefits which must guard against the security concerns.

Software coding, developing, security and design are important factors to keep work in security posture, also network intrusion logs and other logs which save information about who is sharing and using the infrastructure. Operational areas must be fully controlled with analysis of every strange activity which may help to detect any unknown attack.

Cloud customers must know everything about the features and functionality of services and infrastructure as the internal security procedures, configuration, patching, auditing, and logging, how data and related logs are stored and who has access to them.

Virtual machines cannot provide full security or protect the system against attacks by itself.

Cloud computing customers use a shared technology with the efficiencies and risks of virtualization, shared technology used by multiple customer needs to locate physical resources known by customers.

5. VIRTUAL PRIVATE NETWORK (VPN) [3]

A. Definition and Types

There are several definitions for the VPN. For this research we adopted the Microsoft definition which defines it as" a point-to-point connections network, such as, the Internet, and the clients or the users use a protocol, such as TCP/IP, to make virtual calls to VPN server". Fig. 2 shows a VPN.

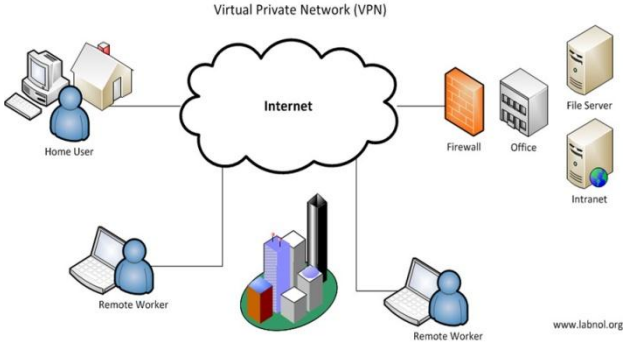

Figure 2. Virtual Private Network VPN

There are also several types of VPN [28], Table (1) summarizes these types and their main features.

TABLE 1. VPN TYPES & FEATURES

VPN Type	Main features
Point to Point Tunneling Protocol (PPTP)	Has some issues of safety for not having strong encryptions, but recommended for normal data or information exchanges.
Layer Two Tunneling Protocol (L2TP)	It has not any encryption methods by itself because it just provides tunnel over in TCP/IP layer two. Used in SP's ADSL connection. Also many providers use it because it is easy to implement and easy to give a good support for any kinds of compatible systems, devices, and the internet.
Internet Protocol Security VPN (IPSec VPN)	The most used VPN type these days because it provides better security for data comparing to the PPTP. IPSec works on Layer three in OSI model to support the excellent safety in peer-to-peer or point to point. Used in Windows, Linux, Apple Mac., and Smartphone operating systems.
Secure Socket Tunneling Protocol VPN (SSTP VPN)	It is used in Windows OS, and gives the Windows users a very high level of security and used in standard of "https" for best usage in any infrastructure. It also can be used with firewalls or web proxy to pass the blocking issues.
Open VPN	PCs OS as Windows and Linux has easy ways to use Open VPN client installation software and can be found in internet for free. But smart devices OS as Android or IOS must be rooted or jail broken to install open VPN apps for free to get SSL VPN from a third party.

When you want to use any remote networking solution as VPN you need to facilitate controlled access to corporate resources and information, allow users to use and connect to LAN resources and to each other, and must ensure the security of data over the Internet. Also use other methods for sensitive data transferred over internet or work network. [7]. Therefore VPN should support the following functions:

1. User Authentication. It must verify the client's identity and establish if he / she is authorized to access to the VPN because only authorized users can accessed to the VPN.
2. Address Management**.** It must assign an address on the intranet and ensure that address is private.
3. It must regenerate every time keys of encryption for the client and server.
4. Multiprotocol Support. It must handle many protocols used in the public network.

B. Secure Sockets Layer (SSL) VPN

There are many definitions of the SSL VPN, Northwestern University Information Technology (NUIT) defines it as a service that allows clients to access remotely, restricted network resources by using secure path and authenticated methods to encrypt all traffic and provide the appearance that clients are in the local network. It is also compatible with any of the platforms, firewalls, to provide a reliable connection [8].

Cisco also defines it as an emerging technology to remote-access VPN capability, by using the Secure Sockets Layer function which is built into a web browser. It also allows clients from any location to access, thus promising productivity enhancements by web browser to improve availability; IT cost reduction software and support. [9].

Techopedia website defines it as a service that allows remote clients to access client-server network or intranet without having to install specialized software on their computers. [10].

Reference [11], there are two major types of SSL VPN, these are:

a) **SSL Portal VPN**: A single SSL that connects to websites which allows the end users to access multiple services securely. Users access it with any Web browser with authentication methods.

b) **SSL Tunnel VPN**: Using the web browsers to access networks services securely as non-Web based protocols. It requires that the Web browser provides functionality which is not accessible through the portal.

c) While12], classify VPN into four types, these are:

d) The clientless SSL VPN. In these types of SSL VPN the client has to install software on their device as web browser which must support SSL without installing some extra function as ActiveX controls or Java.

e) The semi-clientless SSL VPN. In these types clients are also using a normal type of Web browser but they should install some add-ons like ActiveX or Java, to access other types of applications which do not use web as Outlook.

f) The client-based SSL VPN. These types require software to be installed on clients PCs to interact with. Users will access the network as LAN but not all protocols are supported.

g) The full network access SSL VPN or true VPN. These types of SSL VPN seem like IPSec VPN but with encryption and tunneling. They use UDP protocol instead of TCP protocol due to sync issues that would present problems with TCP and this type could be used in remote access services.

SSL VPN should support the following functions:

1. Centralized security and management. It uses a single point of connection for all remote access traffic.
2. Strong and scalable data encryption for maximum Security.
3. Scalability: measured in number of users of providing appliance and throughput (Mbps or Gbps).
4. Endpoint Security.
5. Roaming or Mobility.
6. RF monitoring and planning to avoid dead spots (holes in Wi-Fi coverage). There are tools to help efficiently position wireless access points (APs) and detect sources of RF interference.
7. Rogue access point detection, Rogue Access Point detection is one of what some vendors of

WLAN refer to as “securing the air”

C. Mobile VPN

In the last few years many users use mobile phones and tablets to access the internet and to do their work, so they are looking for VPN connection on their devices OS like Android or IOS. [13]

A specific step can be followed to configure T PPTP VPN in the OSs of these devices as shown herby:

I) Configuration on IOS Devices

1. Go to “Settings”, select "VPN" and Add VPN.
2. Choose ‘PPTP’, and add your VPN (server name, VPN username, Password).
3. Put the Secure ID into (OFF).
4. Save the VPN configuration.
5. Switch VPN status into ON, wait until VPN is connected.
6. Insecure interfaces APIs and software access: Cloud service providers

II) Configure PPTP VPN in Google Android Devices

1. Go to “Settings”, select "VPN" and (+) to Add VPN.
2. Your VPN (server name, VPN username, Password,)
3. Set type of VPN in "PPTP"
4. Put the Secure ID into (OFF) and Save the VPN configuration;
5. Switch VPN status into ON, wait until VPN is connected.

D. Routers Definitions and Types

A router is a physical device that connects and joins two or more networks together. Technically, the router works with Layer 3 gateway which means that it connects two or more networks and that the router operates at the network layer of the OSI model. [14].

There are many types of routers used in data centers of organizations, but we will talk about home or small business that has two types, with many differences and functions. [15].

I) Broadband Routers: Broadband routers are used to do many different things. They are used to connect two or more computers in the same network to other networks that contain two or more computers to create a single network and connect it to the Internet. They can be used to create a voice connection. If using Voice over IP (VoIP) technology, you need a router to connect your

phone to your internet line. The special types of internet modems have both Ethernet "RJ-45" and phone jack [15].

II) Wireless Routers: Wireless routers are used to connect your devices to your modem and create a wireless network in the home or office. So, any device that includes computers, mobiles and tablets within the Wi-Fi range can connect to the router and use the Internet. The best way to keep your network safe from unauthorized connections is to secure your router [15].

E. Firewall Definitions and Types

The firewall is a set of software based in the network gateway server. It protects the private network from users from other networks. Firewalls work with a router program, to test each packet transferred within the network to forward it toward its destination. It also includes a proxy server.

It is installed in many places in the network, in computers as an application and in servers as a hardware.

There are several types of Firewalls:

1. Packet Filter: It looks at every sent or received packet to the network to approve or reject the packet which depends on user's rules. Packet filtering is effective and transparent to users and it is difficult to configure.
2. Application Gateway: It applies a mechanism of security to specific applications as Protocol and Telnets and it is effective but it can decrease the performance.
3. Circuit-level Gateway: It applies a security mechanism when using a TCP and UDP connections.
4. Proxy Server: It intercepts all messages sent or received in the network. It effectively hides the true addresses.

F. Short Message Service "SMS"

Short Message Service (SMS) is a text messaging service used by mobile phone, web, or smart device systems. It uses communication protocols to allow telephone lines or mobile devices network to send and receive the short text messages. [16]

The term is used for any type of short text messaging or user activity itself in many parts of the world. SMS is also good for marketing and it has been used by governments, universities and many companies, also known as SMS marketing.

SMS also used to be a new way to authentication as a delivery channel for a one-time password generated by information systems. In SMS user authentication, the user receives a code or password by a message in the cell phone, reads it and types back the password or code to complete the authentication.

The identification of mobile number effectively enables the cell phone owner to possess an authentication with him, so the user registers in any information system and uses his mobile number with different applications and uses SMS authentication to authenticate that he is the right user, so SMS is an effective service used in means for places by mobile phones and can be used in the community [17].

SMS can be used as an authentication mechanism for protection against the "man-in-the-middle") attacks. If the "man-in-the-middle" use of a fake website to bank, mail server and information system gateway in the Internet to intercept sensitive information, SMS can be an out-of-band mechanism to confirm the authentication. As the "man-in-the-middle" it is impossible to obtain the SMS information through the Internet, the attack will become unsuccessful.

The one-time passwords (OTPs) are a code sent by (text message). SMS offers the convenience of using a mobile phone while adding the security of out-of-band delivery. Mobiles are one of the few devices most people already actively protect. With OPTs there is no need for companies to own, distribute or replace standalone delivery devices. [18].

OTPs are friendly to end users and are a true out of band delivery. MITM and other attacks can attack the user over the internet infrastructure if he receives the message over email, so internet infrastructure can intercept the user and code server, but while delivering OTPs over the mobile network it is unable to intercept delivery of the password.

6. THE PROPOSED SYSTEM

A. The Typical Cloud Access

The following steps are typically followed to access the cloud in a standard way, as shown in Fig. 3

1. Access to the web server from any device.
2. Insert the ID and Password in login page.

3. Getting the permission to access to the cloud service.

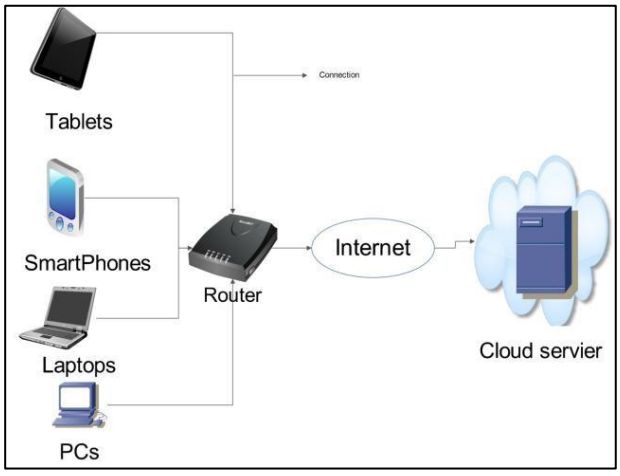

Figure 3. The Standard way to access to the Cloud

B. Insecure, and secure Interfaces

Cloud service providers provide many interfaces or APIs "application programming interface" software used by customers to interact and manage their cloud services. The ***insecure*** interface is any public interface used by anyone to access to the cloud, as web browsers.

C. The Typical Secure Interfaces

I) The Typical Secure Interfaces:

The standard secure interface is a private application that can be used to access the cloud. The cloud can be accessed by mobile devices through VPN connection to log in to the private application. Using the VPN technology with IDs and passwords to authenticate the access from different types of devices, as shown in Fig. 4, the application must be installed only on the user's devices. Then, the following steps are followed to complete the access:

1. Make a connection between the device and the private network by using VPN.
2. Insert the ID and Password in login page of the VPN connection
3. If VPN connection is accepted, open to the private application installed on the mobile device.
4. Insert the ID and password in the login page of the cloud.
5. Access to the cloud service is granted.

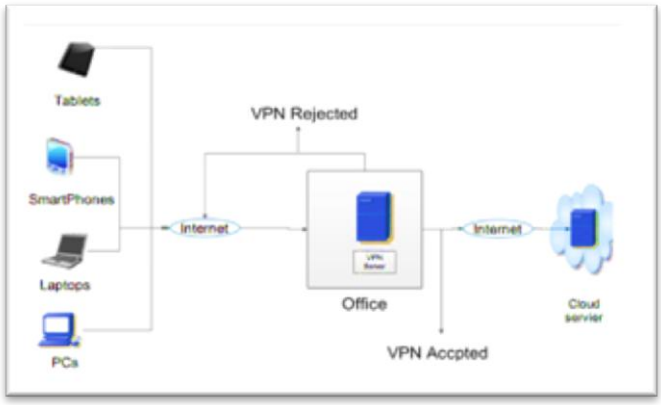

Figure 4. Accessing the Cloud through Typical secure interface

II) Our Proposed Security Enhanced Interfaces:

The cloud can be accessed by mobile devices through VPN connection and SMS server that is based in the user mobile and send an authentication SMS message with confirmation number to login with any web browser, as shown in Fig. 5. The following are the steps needed to be followed in our proposed system that uses an SSL VPN.

1. Make a connection between the device and the private network by using SSL VPN.
2. Insert the ID and Password in login page of the SSL VPN connection.
3. If VPN connection is accepted, access the cloud by typing the cloud address on your web browser.
4. In the login page of the cloud page, access the cloud using your user name and password.
5. You will receive an SMS message on your Mobile with access code.
6. Insert the code you received in the cloud login page.
7. Then you will be granted access to the cloud service.

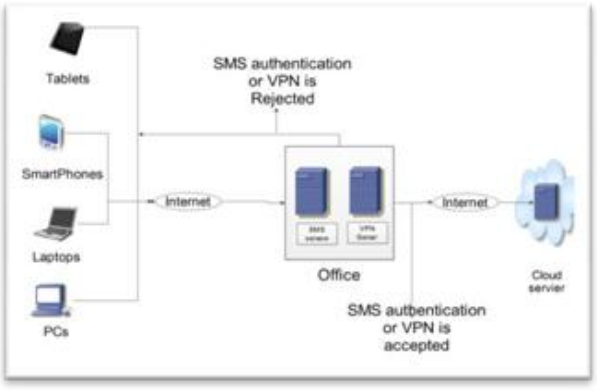

Figure 5. Accessing the Cloud through SSL VPN and SMS System

Our proposed secure interface has been implemented and tested successfully. The implementation requires the following devices:

1. A firewall.
2. Internet router (configured as bridge).
3. Computer device (as web server).
4. SMS Authentication service.
5. Sharing file systems work on web browser (programmed by asp).

E. Result

The result that research find after implementing the proposed system using SSL VPN and SMS service:

1. VPN is important to create a secure connection.
2. SMS code is important to make sure that the user is authenticated and allowed to access to the cloud from mobile devices.
3. No one can access the system if he is unauthorized.
4. The SSL VPN connection is compatible with the 1st gate to the cloud when using secure or insecure interface.
5. Most mobile devices can be configured with VPN and cloud environment.
6. The SSL VPN and SMS solution is lower cost than creating apps for smart phones and tablets.
7. Insecure connection (web browser), will access 1st to private VPN (SSL VPN) before access to the cloud, (the device will access the VPN to get the authorization to access the cloud).

CONCLUSION

In this paper we first introduced the main concepts of the elements that compose our proposed system to secure access to the cloud services. These are, cloud computing, the threats to cloud computing security, the VPN, and the other tools required to implement the system. Then we described the structure of the standard way of accessing the cloud and the structure of the proposed system. Finally we described the steps required to implement the proposed system. The system was successfully implemented and tested.

REFERENCES

1. Dirk C. Aumueller, "IT-Compliance Analysis for Cloud Computing", a thesis submitted for graduation to the academic degree Master of Science (M.Sc.), University of Applied Sciences Darmstadt, Faculty of Computer Science, 16 August 2010.
2. Cloud Security Alliance, "Top Threats to Cloud Computing", Vol 10, March 2011.
3. Michelle Miley, "What Is VPN?", eHow Contributor , last updated April 2012.

   http://www.ehow.com/about_4671848_what-is-vpn.html.
4. http://chandrus.wordpress.com/2013/05/07/a-brief-history-of-cloud-computing/.
5. http://blog.appcore.com/blog/bid/167543/Types-of-Cloud-Computing-Private-Public-and-Hybrid-Clouds.
6. http://www.exforsys.com/tutorials/cloud-computing/cloud-computing-security.html.
7. http://technet.microsoft.com/en-us/library/bb742566.aspx.
8. http://www.it.northwestern.edu/oncampus/vpn/sslvpn/.
9. http://www.cisco.com/web/about/security/intelligence/05_08_SSL-VPN-Security.html.
10. http://www.techopedia.com/definition/17006/secure-socket-layer-virtual-private-network-sslvpn.
11. http://www.techopedia.com/definition/17006/secure-socket-layer-virtual-private-network-sslvpn.
12. http://www.techrepublic.com/article/solutionbase-introduction-to-ssl-vpns/5647244.
13. http://whyvpn.org/mobile-vpn/.
14. http://compnetworking.about.com/cs/routers/g/bldef_router.html.
15. http://whatismyipaddress.com/routers.
16. http://en.wikipedia.org/wiki/Short_Message_Service.

17. http://www.eauthentication.gov.hk/en/professional/sms.htm
18. http://www.authentify.com/solutions/sms.html

Dr. Adeeb Hamdoon Sulaiman has a PhD. in Computer Science from University of Newcastle Upon-Tyne, U.K., 1984. Currently he is a programme leader for the Bachelor Degree of Management Information Systems (MIS) at the Applied Science University/Kingdom of Bahrain. He has held several academic positions including Assistant College Dean, Head of Quality Assurance Unit, Head of MIS department, Head of Computer Science Department, and faculty member in several different institutions in different Arab countries including Iraq, Jordan, Oman, Sudan, and the Kingdom of Bahrain. He has supervised more than 30 M.Sc. students in the different fields of Information Technology. He has published 16 papers in the areas of Data and Computer security, Algorithms design, E-Commerce, and one paper in the quality assurance field. In addition to his academic experience, he has occupied th position of the Head of Computer Center and he has been involved in several information systems projects.

PhD. in Computer Science, Loughborough University of Technology, U.K., 1986.
MSc. in Computer Science, University College London, London University, U.K., 1977.
BSc. in Mathematics, College of Science, University of Baghdad, 1970.
Professor Hilal Mohammed Yousif Al-Bayatti joined Applied Science University as the Vice President for Academic Affairs and Development in September 2007. As a Vice President for Academic Affairs and Development, he is responsible for providing academic leadership to the university. The positions reporting to him include 3 College Deans, Dean of Student Affairs, Dean of Research and Postgraduate Study, the University Librarian, and Director of Academic Staff Development Unit. Professor Al-Bayatti was appointed as advisor to the VP Academic Affairs and Development on September 2015.

Professor Al-Bayatti graduated from the College of Science, University of Baghdad in 1970, with a Bachelor Degree in Mathematics. He then obtained his MSc in Computer Science at the University College London, University of London in 1977. He later obtained his PhD in Computer Science at Loughborough University of Technology in 1986.

Professor Al-Bayatti was promoted to Associate Professor in 1992 and to a Professor in 1998. Professor Al-Bayatti has held a number of Academic and Administrative positions at department, faculty, and university levels. He was appointed to the post of Head of Computer Science Department from 1992 to 1994, and to the post of Dean from 1994 to 2005. He was appointed to the post of Vice President for Academic Affairs and Development at ASU in September 2007.

As an academic, Professor Al-Bayatti's research interests lie in Computer Science as well as Computer and Information Security. He has published over 50 scientific papers and book chapters. Professor Al-Bayatti acted as a peer reviewer, and a member of editorial boards of many scientific journals. He supervised over 60 PhD/MSc students to completion.

Ahmed Mohammed Bayouni: Hold a Master degree and Bachelor degree in Management Information Systems from the Applied Science University/ Kingdom of Bahrain. He has attended several Information Technology training courses and obtained certificates in CCNA, A+, N+, data security, database , and strategic Technology planning from India, Kingdom of Bahrain, and Saudi Arabia. He is currently working as a consultant for local and international information technology companies in Saudi Arabia. Last year, he cooperated with AL Eqtisadia newspaper as a technology journalist and column writer.