Implementing Cloud Computing
With Security Features On
Electronic Libraries

Dr. Shakir Naji Mahmood
Assistant Lecturer Ali yahya Ghani
College of Education-Ibn Al-Haitham
University of Baghdad
Implementing cloud computing...

Abstract
Cloud computing is a style of infrastructure where capacity, applications, and services (such as development, maintenance, and security) are provided by a third-party provider over the internet often on a “fee of use basis”.
The users go to the web for the services by need.

Cloud computing models vary: infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Manage the cloud computing level via surrounding management layer.

Electronic library was built in 2008 in the department of computer science in college of Education for pure science/Ibn Al-Haitham-University of Baghdad.

The researchers will discuss the cloud computing models, Characteristics and how they are implemented on the electronic library in the department of computer science in college of Education for pure science/Ibn Al-Haitham-University of Baghdad and how cloud computing can improve this organization.

As any technology, there is a limitation with cloud computing technology; one of the major problems with the cloud computing technology is data security. The researchers will implement an access control service as a solution for this problem in this research.

Finally, the researchers come up with Aguide can help to choose a secure account that’s hard-to-crack.

Keywords: infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), service oriented architecture (SOA), Access control.
Introduction

The “cloud” in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces, that combine to deliver aspects of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the internet (either as separate components or a complete platform) based on user demand [1].

Cloud computing has been a hot topic over the years amongst IT professionals. “Cloud computing represents the confluence systems, and applications that have evolved over the past few decades” (Lin at al. [2]), as sown in figure (1).

The researchers will discuss the cloud computing models, Characteristics and how they are implemented on the electronic library in the department of computer science in college of Education for pure science/Ibn Al-Haitham-University of Baghdad.

The researchers will highlighting on some limitations and strength points of this new technology, and find the solutions for the limitations and problems for it.

Also, the researchers will come up with a guide can help to choose a secure account that’s a hard-to-crack.

Cloud computing models

- **Infrastructure as a Service (IaaS).** The IaaS layer offers storage and compute resource that developers and IT organization can use delivers business solutions [1].

- **Platform as a Service (PaaS).** The PaaS layer offers black-box services with developers can build applications on top of compute infrastructure. This might include developer tools that are offered as a service to build services, or data access and database services, or build services [1].

- **Software as a service (SaaS).** In the SaaS layer, the service provider hosts the software so you don’t need to install it, manage it, or buy hardware for it. All you have to do is connect and use it. SaaS Examples include user relationship management as a service [1].

The researchers suggest subscribing to these three models to improve the electronic library in this research, as shown in figure (2).

Types of clouds

Cloud computing happens on public cloud, private cloud, or hybrid cloud. Governance and security are crucial to computing on the cloud, whether the cloud is in your organization’s firewall or not.

- **Public clouds** are virtualized data centers outside of your organization’s firewall. Generally, as a service provider makes resources available to companies, on demand, over the public Internet [1].

- **Private clouds** are virtualized cloud data centers inside your organization’s firewall. It may also be a private space dedicated to your company within a cloud provider’s data center [1].

- **Hybrid clouds** combine aspects of both public and private clouds, which are used in this research [1].
Cloud computing characteristics
According to IBM [3, 8], Cloud computing, whether public, private or a combination, will typically demonstrate the following technology features:

- Services focused
- Shared, highly scalable, networked infrastructure
- Automated service delivery
- Enhanced, standardized user experience

Services Focused- The concept of cloud computing is about providing services to any authorized User, anywhere, from using any device. As a result, cloud computing must be built on a service Oriented architecture (SOA), and it has to be deployed in comply with best practices of service Management. According to IBM [3, 8], the Chairman Emeritus, Irving Wladawsky-Berger, IBM Academy of Technology has stated, “SOA is to cloud computing as HTML is to the internet.”

Shared, highly scalable, networked infrastructure- A highly standardized, efficient, shared, Virtualized servers, storage, network, data, middleware, applications, and business process in a layered model known as stacks of cloud services. This can be rapidly scaled up and down with elasticity through automated workload management in secure way to deliver high quality service.

Automated service delivery-Cloud computing helps business process, applications and IT Infrastructure in a collaborative way by providing automated service delivery. It can allocate service, dynamically move and optimize workloads and data across the shared IT infrastructure. These resources are returned to the cloud and are immediately made available to others when they are no longer needed. The service management supporting the cloud service also tracks usage for purposes of billing or usage chargeback.

Enhanced, standardized user experience- Easy-to-use interfaces and straightforward information access are provided to the user to fulfill his or her computing requirement.

Research problem
One of the major problems with the cloud computing technology is data security threats:

- Confidentiality: If you are providing your data to a third party, you have no control over it, how can you assure the confidentiality of data?
- Integrity: How well the data is being secured to protect from tampering and what is the Chance of leakage.
Availability: Cloud computing provide a better backup than most of the companies, but this Technology heavily depends on internet. If ISP fails all access to your data is failed.

Access control

Access control, by the broadest definition, is the ultimate goal of all network security; granting access when appropriate and denying when inappropriate [4]. Similarly, access control is often the goal of physical security; a security guard may grant you entry to the public area of a private bank, but may deny entry to the bank’s safe room. Security guards help enforce physical security, whereas access control methods help accomplish this purpose with network security, as do firewalls and encryption. In light of the true mission of network security, having the right access control methods is absolutely essential. The various types of access control methods enforce security policy and/or users’ privileges by protecting mail server, web applications, database systems, fileservers, applications, or some combination of these resources.

There are many types of access control methods and many non-standardized terms to describe them that it is difficult to determine which solution is right for a given application. An understanding of the more common usage of these terms can make it easier to distinguish between the basic types of solution available.

User authentication is often the primary basis for access control, keeping the bad guys out while allowing authorized users in with a minimum of fuss. In the cloud environment, authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. [5]

Security of computer systems is conventionally achieved via protection and assurance. The former is usually provided by some security subsystems or mechanisms, which are designed to protect the system from specific threats. A threat is any potential occurrence that can have an undesirable effect on the assets and resources associated with a computer system. Protection is based on the premise that it is possible to list most of the threats which can happen, and to build mechanisms that can prevent the threats [6]. Assurance refers to the confidence that the security enforcement is appropriate [7].

A Guide to choose a secure password to access

For almost every account that people make online, they are required to make a secure password. Choosing one that people can't figure out is a matter of creating unlikely letter and number combinations. Here is a guide on how to make a hard-to-crack password [10].

- **The length of password.** We create a password that has eight or more characters since this is usually the minimum for most password requirements. The longer the password the more secure it is likely to be.

- **Form a "random" sequence of words and/or letters.** We create a phrase or series of letters that is seemingly "random" but is easy to remember. Call this your "base-word."
  Example: My children are Jessie, Cassey, Michael and Jenny, so my base-word becomes “jecamije".
• **Add numbers to the base-word to make it more secure.**
  Example: Add the ages of the children to the end making it "jecamije22191612".

• **Use punctuation and symbols to "complicate" it further.**
  Example: Add a symbol to the word to make "houseonspooner#1500".

• **Create complexity with upper and lowercase letters.**
  Example: Take advantage of adding capital letter to create "JeCaMiJe22191612".

• **Generate similar but altered passwords.** Use the same or similar base-words to help you remember your passwords easily without making them "too" easy to crack.
  Example: Take advantage of adding capital letter to create "JeCaMiJe22191612".

**Proposed model**

Our proposed model is to generate two Access Control Lists (ACLS) to distinguish between library staff and end-user. The proposed model is using software as a service (SaaS) as a cloud computing model.

**Checking access:**

1. **Library staff who is responsible for keeping the library up to date.** This list (a file) contains the position (Of each library staff) and a password to authorize them to make updating to the library database, and this list can be contained in the updating program and change periodically.

2. **the second ACL is for authorized end-users, showing their names and passwords.** This list is a database contained the names of authorized students to access the library which is stored in the cloud.

**Model Algorithm**

**Step1. Call check access.**

**Step2. Enter the password.** The model checks the validity and the type of user (library staff or end-user) from this password. If it is within the ACLs which stored in the cloud then it will accepted otherwise the model ask to try again (up to three times) then it will be rejected.

**Step3. If a library staff is recognized (authorized), updating to database(s) is allowed.** This will check the integrity of the stored data in the cloud (prevention of unauthorized modification of information).

If an end-user is recognized, accessing only to database is allowed. This will check the confidentiality (prevention of unauthorized disclosure of information).

**The result of implementation**

Electronic library was built in 2008 in the department of computer science in college of Education for pure science/Ibn Al-Haitham-University of Baghdad, contains thousands of books in different fields saved in server with more than 3000GB capacity.

As any technology, there is a limitation with cloud computing technology; one of the major problems with the cloud computing technology is data security. The researchers will implement an access control service as a solution for this problem in this research.

By implementing an access control service to prevent unauthorized from using library resources (i.e., this service controls who can have access to a resource, under
what conditions access can occur and what those accessing the resource are allowed to do)[9].

Cloud computing is a great technology, by implementing it on our electronic library we can achieve:
1. Universal file access.
2. Easier Group Collaboration.
3. Lower cost of hardware, software and maintenance.
4. Pay according to usage.
5. No needs for back up files were programmers spent a lot of time and efforts to make them before.
6. Unlimited storage space.
7. Reliable data storage.
8. Improve computer performance.
10. Reduce the human recourses, which can help to reduce the sum of money which was spent in the organization for their salaries before.
11. 24 hours, 7 days (24x7) support.
12. Secure storage management.

Conclusion
Cloud computing is a dominant services paradigm. Involving in this technology increase rapidly and most of the biggest companies such as Microsoft, and IBM encourage flying to the cloud. This technology in maturity stages and it need more time to be able to provide the services to meet customer requirements.

Implementing cloud computing technology in the electronic library in Education College for pure science/Ibn Al-Haitham can help to get many benefits as we pointed in our research before, this technology really can help and support our college to promote the education in our country.

As any new technology, there is a limitation with cloud computing technology; one of the major problems with the cloud computing technology is data security. The researchers implemented an access control service as a solution for this problem in this research.
References


Appendix

Figure (1) Cloud Computing [2]

Figure(2) Cloud Computing models [1]