Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.7 – 15

RESEARCH ARTICLE

An Advanced Security - A Two-Way Password Technique for Cloud Services

Yogesh Brar[1], Shobhit Krishan[2], Ankur Mehta[3], Vipul Talwar[4], Tanupriya Choudhury[5], Vasudha Vashisht[6]

[1,2,3,4] Undergraduate in computer Science from Lingaya's University, India

[5,6]Assistant Professor in School of CS from Lingaya's University, India

[1] yogeshbrar@gmail.com; [2] shobhitkrishan16@gmail.com; [3] ankurmehta003@gmail.com

[4] vipul.talwar09@gmail.com; [5] tanupriya86@gmail.com; [6] ervasudha@gmail.com

---

Abstract: A model for delivering information technology services in which resources are safely stored and retrieved from the internet through web-based tools and applications, rather than a direct connection to a server. Gathering the resources whenever and wherever is a big issue, for smaller companies, and it is a matter of great concern. Thus, Cloud Computing offers a solution to smaller firms. Using the Internet as the backbone, cloud computing provides accessibility to the end users on "*whenever and wherever*" required basis. This type of electronic system having access to web, allows employees to work remotely. Users here are only concerned with the computing services that he/she has asked for. All the details of approaching this task are kept hidden from the user. The data is secured and stored in massive storage data centre and can be accessed from any device all over the world. Research shows that the architecture of current cloud computing system is central structured one; all the data nodes must be indexed by a master server which may become *bottle neck* of the system. Cloud Computing finds its use in various areas like web hosting, graphics rendering, financial modeling, web crawling, etc.

Keywords: Cloud Computing; Abstraction levels; bottleneck problem; design goals; two-way password procedure

---

I. INTRODUCTION

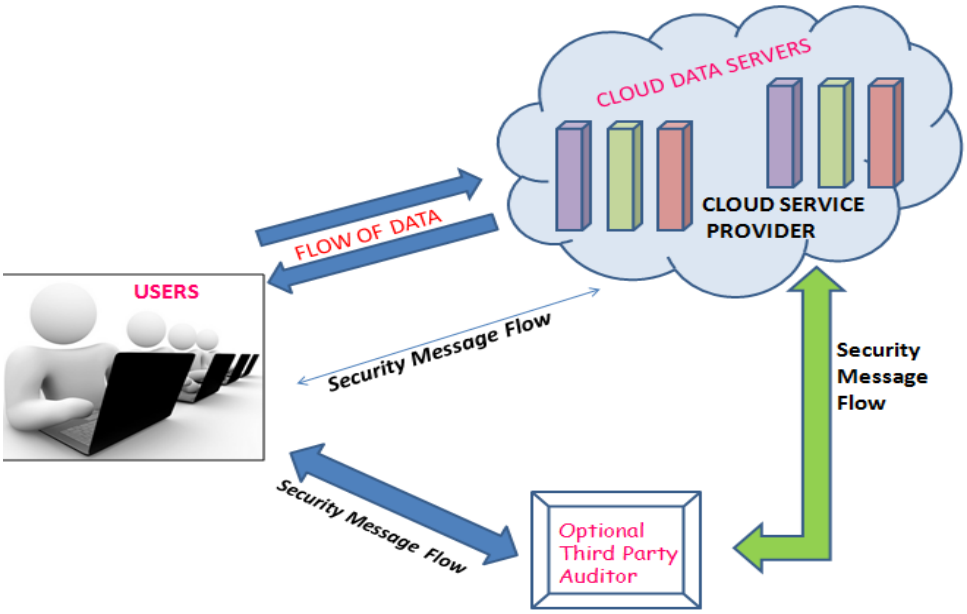
Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing confide remote services with a user's data, software and computation.

II. CLOUD CONCEPT

Clouds are large pools of easily usable and accessible virtualized resources. These resources can be dynamically reassembled to adjust to a variable load (scale), allowing optimum resource utilization. [1]It's a pay-per-use model in which the Infrastructure Provider by means of customized Service Level Agreements (SLAs) offers guarantees typically exploiting a pool of resources. Organizations and individuals can benefit from mass computing and storage centers, provided by large companies with stable and strong cloud architectures. Cloud computing incorporates simulation, on-demand distribution, Internet delivery of services, and open source software. From one point of view, cloud computing is not new because it uses approaches, concepts, and best practices that have already been grounded. From another perspective, everything is new because cloud computing changes how we invent, develop, distribute, scale, update, maintain, and pay for applications and the infrastructure on which they run.

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. It allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by concentrating storage, memory, processing and bandwidth.

Figure 1-



The deployment of Cloud Computing is powered by data centre running in a simultaneous, cooperated and administered manner. Individual user's data is unnecessarily stored in multiple physical locations to further reduce the data integrity threats. Therefore, distributed protocols for storage correctness

assurance will be of most importance in achieving a robust and secure cloud data storage system in the real world. However, such important are mains to be fully explored in the literature.

We generally differentiate the cloud deployment models, by the cloud's infrastructure's provider and its physical location. The three normal cloud deployment models are:

TYPES:

1. **Public Cloud** – People buy the public cloud computing resources from the providers. Mostly, suppliers purchase their existing infrastructure to provide cloud resources at a proportion to support the general public.

2. **Private Cloud** –These cloud computing resources are only feasible to a limited group of consumers, mostly an organization. The cloud substructure may be running in an organization's physical data center.

3. **Hybrid Cloud -** It is a blend of public and private cloud resources. For example, an organization may use its private cloud for its daily operations, and then bring up the level to a public cloud for maximum resource needs.

Figure 2 depicts the relationship between public, private, and hybrid clouds.

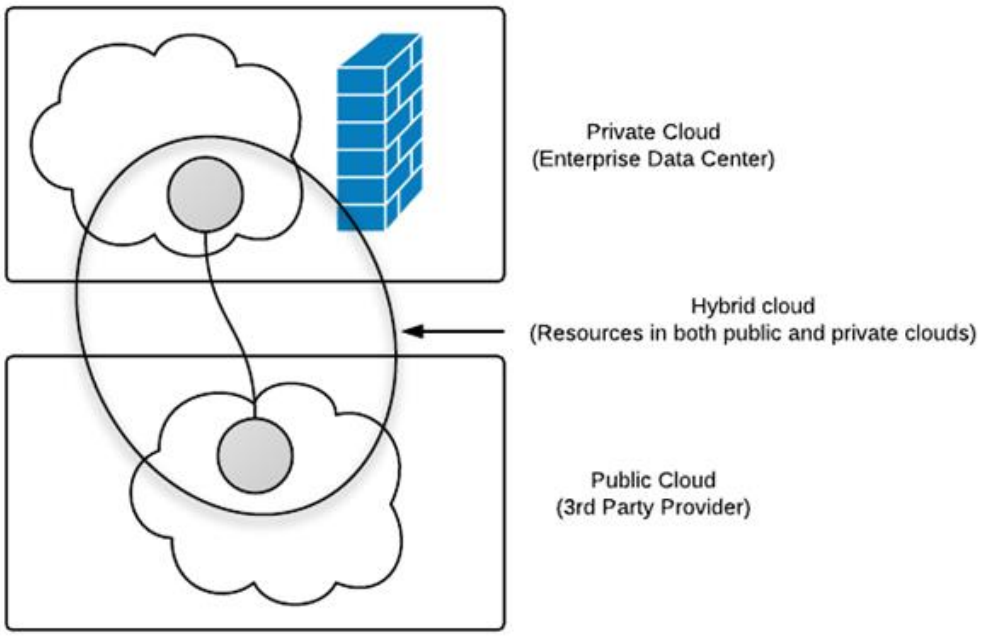


Figure 2 – Cloud Deployment Model

Abstraction of application infrastructure includes several levels, computation abstraction and storage abstraction and also abstraction of all the layers of applications.

[2]The three most normal levels of *abstraction* are:

1. **Infrastructure as a Service (IaaS)** –"*Infrastructure as a Service*" also known as *Cloud infrastructure services*, delivers storage, networking and most importantly the Infrastructure. Here, instead of purchasing the software or the other network equipments, a user can buy the service by simply outsourcing it. Infrastructure as a Service's users are responsible for managing runtime, applications and data and O/S. Vendors however manage servers, storage, and networking.

2. **Platform as a Service (PaaS) -** "*Platform as a Service*" also called as *cloud platform services* is certainly the most composite form of the Cloud Platform Services which delivers computational resources through a platform. It provides the computing infrastructure, the hardware, and the platforms that are installed on top of the hardware thus making the development and testing of applications simple, feasible and fast. With Platform as a Service, vendors still manage runtime, servers, operating systems, storage and network, but here the users manage the data and applications. Application runtimes, messaging infrastructure and databases, are application platform components that are delivered as a service. The public cloud presentation also provides platform services with the Java the Database Cloud Service.

3. **Software as a Service (SaaS)** –"*Software as a Service*" also sometimes called as *Cloud Application Services* are the easiest and the most popular form of cloud computing. Here the applications are managed by third-party vendors and their interface is accessed on the client's side. These applications run directly on web browsers. As everything for example applications, runtime, servers, O/S are managed by the vendors, now it becomes easy for a company or an enterprise to contour their support and maintenance. Famous example for SaaS is Gmail. Delivery of services in this takes place for Business applications, such as email, CRM, HCM, and ERP applications.

The levels of abstraction for these service models are shown in Figure 3.

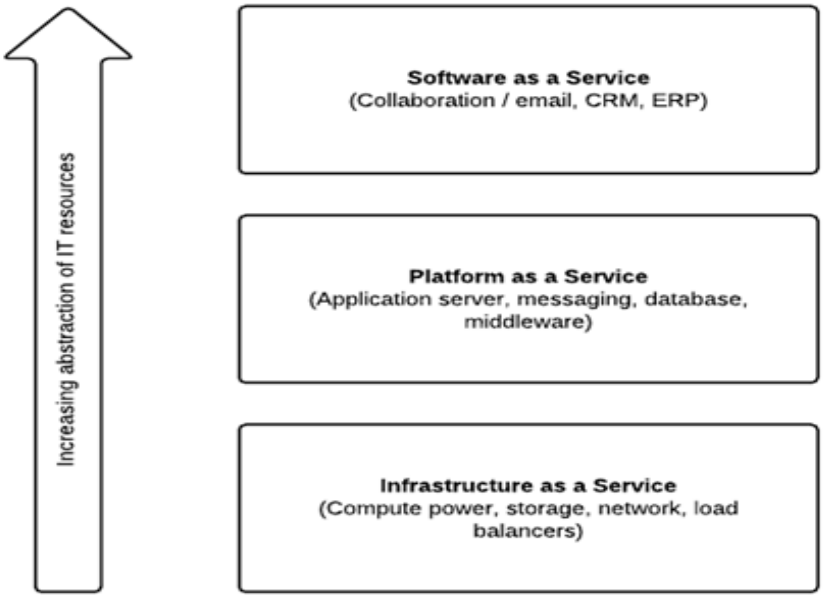


Figure 3 – Levels of abstraction in cloud computing service models

III. PROBLEM STATEMENT

A. System Model

Representative network architecture for cloud data storage is instanced in **Figure 1**. Three different network entities can be identified as follows:

- **User:** Users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

- **Cloud Service Provider (CSP):** A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live Cloud Computing systems.

- **Third Party Auditor (TPA):** An optional TPA, who has expertise and capabilities that users may not have, is trusted to evaluate and expose risk of cloud storage services on behalf of the users upon request.

We consider a cloud data storage service involving three different entities, as instanced in Fig. 1: the **Cloud User** (U), who has large amount of data files to be stored in the cloud; the **Cloud Server** (CS), which is managed by Cloud Service Provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter.); the **Third Party Auditor** (TPA), who has expertise and capabilities that cloud users don't have and is trusted to evaluate the cloud storage service security on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. We consider the existence of a semi-trusted CS does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, during providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or tangled failures to maintain reputation.

B. Adversary Model

Security threats faced by cloud data storage can come from two different sources. On the one hand, a CSP can be self-interested, mistrusted and possibly malicious. Not only does it desire to move data that has not been or is rarely accessed to a lower tier of storage than agreed for [3]monetary reasons, but it may also attempt to hide a data loss incident due to management errors, tangled failures and so on. [4]On the other hand, there may also exist an economically motivated adversary, who has the capability to compromise a number of cloud data storage servers in different time intervals and subsequently is able to modify or delete users' data while remaining undetected by CSPs for a certain period.

Specifically, we consider two types of adversary with different levels of capability in this paper:

Weak Adversary: The adversary is interested in corrupting the user's data files stored on individual servers. Once a server is constituted, an adversary can pollute the original data files by modifying or introducing its own fraudulent data to prevent the original data from being retrieved by the user.

Strong Adversary: This is the worst case scenario, in which we assume that the adversary can compromise all the storage servers so that he can intentionally modify the data files as long as they are internally consistent. In fact, this is equivalent to the case where all servers are colluding together to hide a data loss or corruption incident.

C. Bottleneck Problem

Bottleneck term itself suggests narrow path or congestion. In cloud storage this problem occurs when multiple clients access the same piece of information by accessing the same server, resulting into a load on the server and request-response service becomes slow between the client and server.

Bottleneck is caused by multiple factors, including:

- Hardware components, like CPUs
- Graphical processing units(GPUs)
- RAM memory

To prevent this problem we prefer to use the ***Master-Slave Technology*.** This method efficiently helps in dividing the data of one server station into multiple stations, making one station as "Master Station" which will control all the other station's requests and response activity.
Consider a situation of multiple requests by various clients to master server, which will further transfer them to its respective slave stations. Processing of requests would be doneon each station. After processing of requests, Master Server asks its slave stations that whether they have any data for sending to its client.

D. Design Goals

To enable privacy-preserving public auditing for cloud data storage under the previously mentioned model, our protocol design should achieve the following security and performance guarantee:

1) **Public Auditing**: To allow TPA (Third Party Auditor) to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to the cloud users;

2) **Storage Correctness**: To ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing users' data intact;

3) **Privacy Preserving**: To ensure that there exists no way for TPA to derive user's data content from the information collected during the auditing process;

4) **Batch Auditing**: To enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously;

5) [5] **Lightweight**: To allow TPA to perform auditing with minimum communication and computation overhead.

IV. PROPOSED SOLUTION

Problem could be overcome, using basic security techniques. Let's understand it through an example, consider a user who wants to store his/her confidential data on cloud server of a particular CSP (Cloud Service Provider). All he/she demands is full security of data and any time access of his/her data. Now, he/she has left with no other option than to trust on this CSP. At other end, our user is hesitating in hiring TPA (Third Party Auditor) for the inspection of his/her data on cloud server, because it's not a safe option to review your data in front of a stranger.

Now, CSP has the chance to win its user's trust and making its reputation in market, by proposing a new technique of data security for technical as well as non technical users too. So, it presented the idea of two way passwords.

Two-way password Procedure:

The procedure starts from the signing up of user in CSP's website for the cloud service. The moment, user make his account, he is asked for selecting a scheme. For purchasing the scheme, user have to enter the details of his credit card and its secure code. Cloud Service Provider will confirm the authentication of the user. Once the CSP is satisfied two passwords will be generated (both the passwords are unique). One password is for the CSP employees who are maintaining the data onto their server and other password will pass on to the user for accessing his/her data from server (after the service is provided). The user's data can be accessed through this cloud on entering both the passwords only.

Algorithm for 2-way Password Generation

Step 1: User signing up for service,

CSP checking user's authentication through his credit card details...

Password generation initiates, CSP's Password and User's password generated.

If user is authenticated then provide the cloud service

Else

Got to step 2

End

Step 2: Exit

V. CONCLUSION

Using internet as a backbone, cloud computing has reached to the end users whenever they require or wherever they require. There are many services of cloud in the market but the end user finds it difficult to trust on anyone. For solving the problem of Cloud Service Providers and End User *trust relationship* and to ensure the end user with his *data security*, we proposed the new "Two-way Password Procedure". It is a simple and efficient technique to increase the security of user's data on servers it also empowers the end user providing full control of their data on the servers.

REFERENCES

[1] Tanupriya Choudhury, Vasudha Vashisht, Himanshu Srivastava "A Secure Decentralized Cloud Computing Environment over Peer to Peer", IJCSMC, Vol. 2, Issue Date: April 4, 2013, ISSN 2320–088X.

[2] Vandana Choudhary, Saurabh Kacker, Tanupriya Choudhury, Vasudha Vashisht, "An Approach to Improve Task Scheduling in a Decentralized Cloud Computing Environment" Issue Date: Jan- Feb, 2012, ISSN 2229-6093

[3] Dinesha H.A, Prof. V.K. Agrawal "Multi-level Authentication Technique for Accessing Cloud Services"

[4] Maheswaran.M "Cloud Computing" Seminar Report Cochin University of Science and Technology, Nov, 2008

[5] Supreet Singh, Deep Mann "An Effective Billing in Cloud Computing" IJARCSSE, Issue Date: Feb 2, 2014, ISSN 2277 128X

[6] Ankush Narkhede**,** Prashant Barhate, Ashwini Narkhede "A Study on Organize and Optimize Strategy Using Cloud Computing Platform" Issue Date: June 6, 2013, ISSN: 2277 128X

[7] http://apprenda.com/library/paas/iaas-paas-saas-explained-compared

[8] Pradnyesh Bhisikar, Prof. Amit Sahu "Security in Data Storage and Transmission in Cloud Computing" Issue Date: March 3 2013, ISSN: 2277 128X

[9] Sujay Shaha, Pravin Shinde, Shankar Somatkar, Prof. D.K. Joshi, "Data Storage Security In Cloud Computing" Issue Date: Dec 12-Feb 13, ISSN (Online): 2279-0055

[10] K. Palanisamy "TPA Added Service in Cloud Computing" Issue Date: Nov 2013,

ISSN - 2249-555X

[11] www.Seminarsonly.com

AUTHORS' PROFILE

Yogesh Brar is currently pursuing his Bachelor's degree in Computer Science from Lingaya's University, Haryana, India. He is a Student Ambassador at Mozilla, Deputy Manager at Google Developers Group, Lingaya's University and a Member of Bugsquad & Quality Team at Canonical Ltd. His areas of interests include Data mining & Warehousing, Cloud Computing, Operating System, Arduino, Image Processing.

Shobhit Krishan is currently pursuing his Bachelor's degree in Computer Science from Lingaya's University, Haryana, India. His areas of interests include Cloud Computing, Database management system and Web Development.

Ankur Mehta is currently pursuing his Bachelor's degree in Computer Science from Lingaya's University, Haryana, India. His areas of interests include Cloud Computing, Web Design.

Vipul Talwar is currently pursuing his Bachelor's degree in Computer Science from Lingaya's University, Haryana, India. His areas of interests include Cloud Computing, Graphic Designing.

Tanupriya Choudhury received his bachelor's degree in CSE from West Bengal University of Technology, Kolkata, India, master's Degree in CSE from Dr. M.G.R University, Chennai, India and currently pursuing his Doctoral Degree. He has two year experience in teaching. Currently he is working as Asst. Professor in dept. of CSE at Lingaya's University, Faridabad, India. His areas of interests include Cloud Computing, Network Security, Data mining and Warehousing, Image processing etc.

Vasudha Vashisht received her bachelor's and master's degree in Computer Science from M.D. University, Haryana, India. She has 6 years of experience in teaching. Currently, she is working as Assistant Professor in the Dept. of Computer Sc. & Engineering at Lingaya's University, Faridabad, Haryana, India. She has authored 10 papers and her areas of interests include artificial intelligence, Cognitive Science, Brain Computer Interface, Image & Signal Processing. Currently she is pursuing her doctoral degree in Computer Science & Engineering. She is a member of reputed bodies like IEEE, International Association of Engineers, International Neural Network Society, etc.

