A^3 (Authenticate Auditor & Avail) for Preserving Integrity of Data in Cloud Computing

Sagar Shivaji Sawant[1], Suhit Sukhadeo Kalubarme[2]

Abstract

Cloud computing is a technology that allows anyone connected to the internet to use hardware & software on-demand. Cloud computing provides services in three different models: Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Deployment Models (Public Cloud, Private Cloud, Community Cloud, and Hybrid Cloud). In Cloud Computing, users can remotely store their data into the cloud & access the data on-demand. Data is stored & maintained remotely by Cloud Service Provider (CSP). Cloud user has no control over the data. Data integrity is one of the most critical issue in the cloud computing. This paper proposes two fundamentals requirements to protect the data from unauthorized access: 1) Third Party Auditor (TPA) scheme to monitor the data available on the cloud server and to protect cloud user from accessing invalid data (Modified data by the Cloud Service Provider for their sake, without concerning Cloud User). We consider TPA to work on behalf of the Cloud User, to verify the integrity of the data store in the cloud. A TPA who has more knowledge, experienced and resources to audit the integrity of data placed onto the cloud. 2) Unauthorized users or hackers should not pretend as TPA, because TPA is trusted party for the Cloud Users, however problem may arise when attacker impersonates as a TPA. We rectify this problem by using the RSA implementation.

Keywords

Cloud, Encryption, Hashing, Integrity, Impersonation, TPA.

1. Introduction

Cloud Computing is a concept where Cloud Service Providers (CSP) offer services using their network of remote servers hosted on the internet to store, manage, and process data, rather than a local server. Then, the cloud user can access their data from any devices or geographical location with an internet connection – wherever and whenever the user needs their data. Cloud Service provider offer services that can be categorized into 3 types.

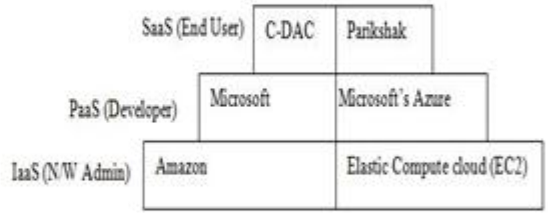


Fig.1: Introduction of Cloud Service Model

Software as a Service (SaaS):- SaaS provides service as software's where Cloud User can access it with the help of internet and browser. It removes the need of installation, maintenance & upgradation of software at local machine. e.g. students can compile the programs (C,C++,Java etc…) online without installing software's on local machine. SaaS is software that is owned, delivered, and managed remotely by one or more providers which is offered as a pay per use service [1]. SaaS is intuitive software that helps, elevate user acceptance and overall customer service

Platform as a Service (PaaS):- PaaS provides service as platform (Programming tool, operating system etc…) to the Cloud User for developing new applications. PaaS provides capability that scale can be specified via configuration file and provided automatically by the environment. Configuration file contains scaling up & scaling down requirements needed in future. In PaaS Developer upload their application code to a platform which is then managed by the Cloud Service Provider [2].

Infrastructure as a service (IaaS):-Infrastructure as a service (IaaS) refers to the renting of computer hardware (servers, networking technology, storage, and data center space) instead of buying and installing it in your own data center. The client need not purchase the required servers, data centre or the network resources. IaaS vendors use virtualization technologies to provide more scalable computing resources. Virtualization it is the process of creating Virtual Machine (VM) which is replica of physical machine. Hypervisor is the main component of the Virtualization process. Amazon's Elastic Compute cloud (EC2) and Simple Storage Service (S3) provide highly scalable on demand infrastructure for running websites and rich applications [3].

According to the report "Assuring the Security Risks of Cloud Computing" published by Gartner, they summarize that there are seven potential security risks around cloud computing services [4] such as: privileged user access, regulatory compliance, data location, data segregation, recovery, investigation support and long term viability. We divide these security risks into the following three aspects according to their different contents [5].

1. Data transmission and storage security
   Around the cloud services environment, Data users send data to service providers mainly through the network. User's personal data, including financial bank information, and other private data, which needs to be secured by several secure transmission modes such as: Secure Socket Layer (SSL), Point to Point Tunneling Protocol (PPTP), Virtual Private Network (VPN) and so forth.
2. Data audit securityWhile transferring data between users and service providers, it is difficult to avoid malicious attack.
3. Security risk preventing strategiesService Level Agreement (SLA) between users and service providers is a useful solution to reduce the security risks. It is one of the cloud computing services advantage. But difficulties that while dealing with issue it will slow down development of cloud computing applications.

2. Data Purity (Integrity) and Impersonation

Data Purity (Integrity)
Integrity of data means to ensure two things: assume Sam sends data to Suzy. First, Suzy must know whether or not the data originates from Sam. For instance, if an intruder pretends to be Sam and sends some data to Suzy, he would know that it is not coming from Sam. Secondly, Suzy must know whether or not the data has been tampered with by an intruder on its way. One of the biggest issues in cloud computing is data stored in the cloud is not verified by server, which is not trusted. This experience Byzantine failures [6] occasionally, may decide to hide the data errors from the clients for the benefit of their own or for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. Integrity of data inside cloud is necessary.

Security Issues: - [7]
Following are some industry examples of such cases:

- Google Docs found a flaw that inadvertently shares users docs in March 2009
- A Salesforce.com employee fell victim to a phishing attack and leaked a customer list, which generated further targeted phishing attacks in October 2007.

Impersonation Attacks
Impersonation can be defined as "copying the behaviour of or pretend to be (another person) in order to deceive". [8] Three different actors are in picture of Impersonation attack: The first actor is the CSP P of some online service like an online bank, an online trading platform (like eBay or Amazon), an Internet Service Provider. The second actor is the Cloud User V, a registered user of the service provider by P. To ensure only authorized access to its services, P performs authentication prior to granting access to its services. For this reason, P has granted V authentication credentials c after registration. Using c it is possible to authenticate as user V toward P. The third actor is the Attacker A. The goal of A is to enjoy the service of P in an authorized way. More specifically, A wants to use P's service by pretending to be V. To do this, A needs V's credential c. so to mount a successful impersonation attack; Attacker A can extract the identity information of V and pretend as a V and enjoying the services from P.

3. Auditing

Auditing it is the process of knowing unauthorized data access and keeping log of the activity. Auditing in cloud computing can be done in five relevant areas[9] 1.Verification of user: Verify that only approved personnel are granted access to service based on their roles and that access is removed in timely manner upon the personnel's termination of employment and/or change in their roles that does not require the said access. 2. Data Integrity: Sufficiency of the data protection policies, procedures and practices at the Cloud Service Providers as well as the user organization. 3. Technology Risks: Unique risks related to the use of virtual operating system with cotenants. 4. Operations: Access procedures related to incident management, problem management, change and access management in context of use of Cloud

Services. 5. Regularity: Compliance with regulatory requirements over the protection of information. In this paper we mainly focus on third-party auditing mechanism in cloud computing services. While introducing the term TPA, the users, who own the data rely on TPA just for the storage security of their data, do not want this auditing process introducing new vulnerabilities of unauthorized information leakage toward their data security [10], [11]. Here we are preserving the integrity of data without displaying data to the TPA.

4. Proposed system

In the proposed system we implemented Third Party Auditing (TPA) to integrate the data & verify the TPA by following manner:
Here we use data & file term interchangeably

1. Cloud Service Provider uploads the client data on the cloud server. Once the file gets uploaded on to the server immediately hash code will be calculated.
2. The hash code will be encrypted by using the public key of TPA & the hash code will be send to the TPA for the further verification.
3. If the TPA is valid then it will be able to decrypt hash code by using the private key.
4. Once the data is uploaded onto the server it is accessible to the all valid users of the cloud. Whenever needed cloud user will give the request to use the file.
5. As request come for downloading from user, It will send to TPA for checking integrity.
6. TPA will check user request and download the instant hash code for current user request from cloud.
7. After getting the instant hash code of requested file TPA will check whether instant hash code & hash code sent by the CSP at the time of uploading file is same or not. If the Hash codes are same then it allows user to download the file otherwise it is considered that contents of the file has been changed by unauthorized user and TPA is not allowing user to download the file.
8. If the file is valid then user can use the file from the server otherwise file is not accessible from the server.

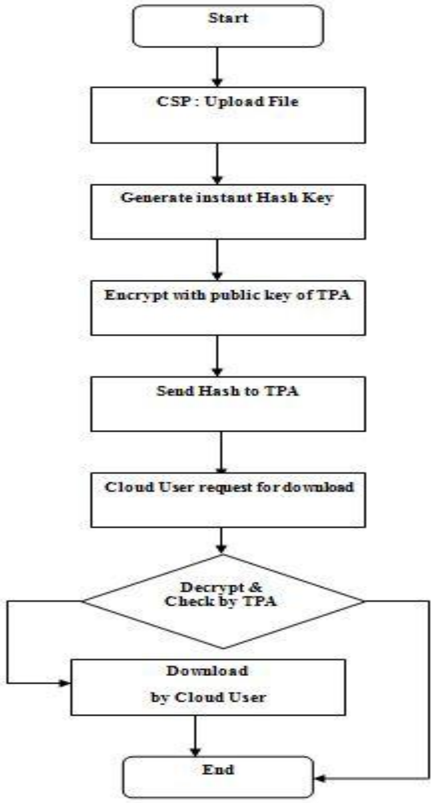

Start
CSP : Upload File
Generate instant Hash Key
Encrypt with public key of TPA
Send Hash to TPA
Cloud User request for download
Decrypt & Check by TPA
Download by Cloud User
End

Fig.2: (Flowchart of Proposed System)

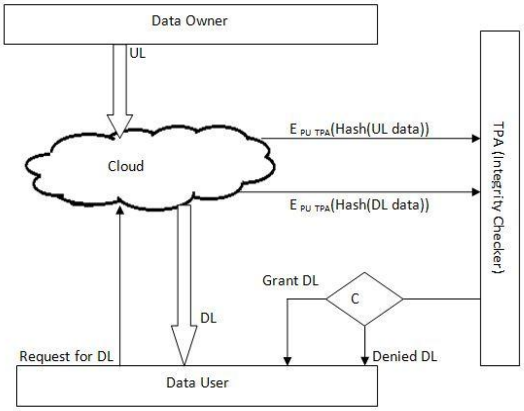


Fig. 3: (Architecture of Proposed System)

1) In proposed system we used AES algorithm for encrypting the data. **Advanced Encryption Standard Encryption technique (Private Key Cryptography):**AES is the new version of 3DES. **Security:** Minimum key size for

AES is 128 bits, brute force attacks with current and projected technology were Institute of Technology) intends that AES shall be available on a worldwide, non-exclusive, royalty-free basis. **Algorithm & Implementation Characteristics:** 1. Algorithm is flexible in terms of key size and block sizes. 2. We can use the algorithm in various ways more efficiently in various applications. e.g. 8 bit Processors, ATM networks, HDTV 3. Stream cipher, MAC & HASH generation are key areas where we can use this algorithm [12].

2) For generating hash code we used MD5. **Message Digest 5:** A hash is a one way function. It is considered a function because it takes an input message & produces an output. It's considered a one way because it's not a practical to figure out what input corresponds to given output & it's computationally infeasible. It is impossible that two message have similar hash value. MD5 hash generation is processing message in 512 bits blocks. Size of MD5 hash is 128 bit quantity. At each stage four passes are require
    1. F(X, Y, Z) defined as $(X \wedge Y) \vee (\sim X \wedge Z)$
    2. G(X, Y, Z) defined as $(X \wedge Z) \vee (Y \wedge \sim Z)$
    3. H(X, Y, Z) defined as $X \oplus Y \oplus Z$.
    4. I(X, Y, Z) defined as $Y \oplus (Y \vee \sim Z)$. MD5 use different 64 constant for each 16 message words in pass 3. No constant for pass one. [13]

3) For authenticating TPA we are using RSA implementation.**RSA Algorithm**: RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. The RSA algorithm involves three steps: key generation, encryption and decryption.

Key generation

With the help of public & private key, we can implement RSA algorithm**.** The public key can be known by everyone and is used for encrypting messages. We can only decrypt the message encrypted by public key, with the help of private key in feasible time period. We can generate PUBLIC & PRIVATE key pair using following way:-

1. Select x & y distinct prime integer number. For security purposes, the integer's *x* and *y* should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primarily test.
2. Compute $m = x.y$. *m* is used as the modulus for both the public and private keys. Its size is measured in bits generally known as key length.
3. Compute $\varphi(m) = \varphi(x)\varphi(y) = (x - 1)(y - 1)$, where φ is Euler'stotientfunction.
4. Choose an integer *e* such that $1 < e < \varphi(m)$ and $\gcd(e, \varphi(m)) = 1$; i.e. *e* and $\varphi(m)$ are co-prime. *e* is released as the public key exponent having a short bit-length and small Hammingweight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of *e* (such as 3) have been shown to be less secure in some settings.
5. Determine *d* as $d^{-1} \equiv e \pmod{\varphi(m)}$, i.e., *d* is the multiplicative inverse of *e* (modulo $\varphi(m)$).
    - This is more clearly stated as solve for *d* given $d \cdot e \equiv 1 \pmod{\varphi(m)}$.
    - This is often computed using the extended Euclidean algorithm.
    - *d* is kept as the private key exponent.

By construction, $d \cdot e \equiv 1 \pmod{\varphi(m)}$. The publickey consists of the modulus *m* and the public (or encryption) exponent *e*. The privatekey consists of the modulus *m* and the private (or decryption) exponent *d*, which must be kept secret. *x*, *y*, and $\varphi(m)$ must also be kept secret because they can be used to calculate *d*.

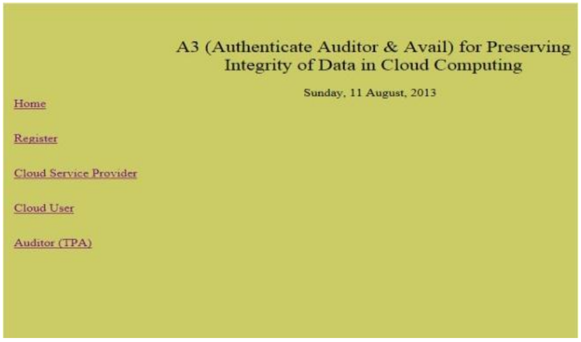
Encryption

- Alice transmits her public key (*m*, *e*) to Bob and keeps the private key secret. Bob then wishes to send message *MSG* to Alice.
- He first turns *MSG* into an integer *msg*, such that $0 \leq msg < m$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text *c* corresponding to
- $C = msg^e \pmod{m}$.
- This can be done quickly using the method of exponentiation by squaring. Bob then transmits *c* to Alice.

Decryption

- Alice can recover *msg* from *C* by using her private key exponent *d* via computing
- $MSG = C^d \pmod{m}$
- Given *msg*, she can recover the original message *MSG* by reversing the padding scheme.

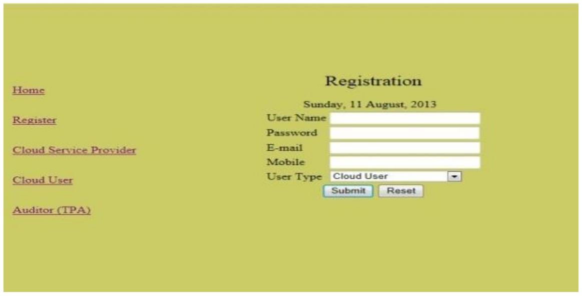
5. Screenshots



A3 (Authenticate Auditor & Avail) for Preserving Integrity of Data in Cloud Computing

Sunday, 11 August, 2013

Fig. 4: Home Page

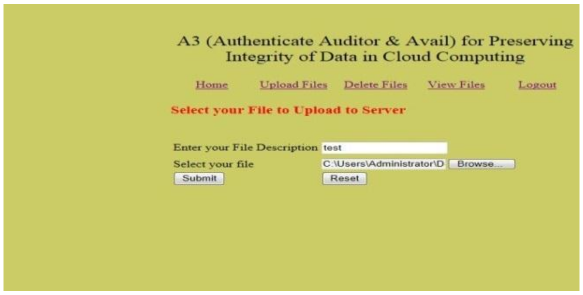


Registration

Sunday, 11 August, 2013

User Name
Password
E-mail
Mobile
User Type: Cloud User

Fig. 5: Registration for CSP & Cloud User

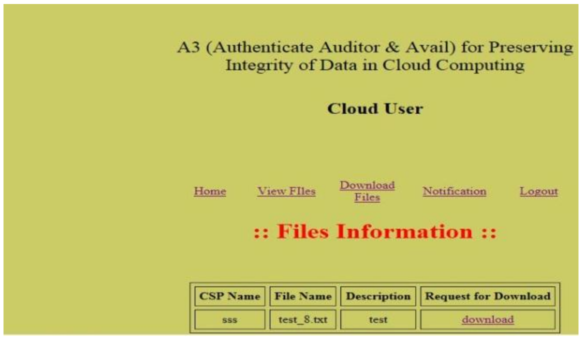


A3 (Authenticate Auditor & Avail) for Preserving Integrity of Data in Cloud Computing

Select your File to Upload to Server

Enter your File Description: test
Select your file: C:\Users\Administrator\D

Fig. 6: CSP will upload file



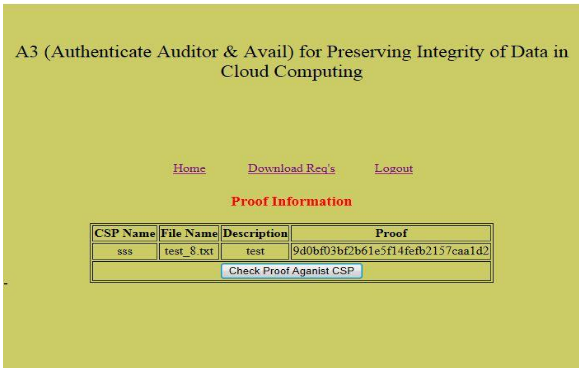
A3 (Authenticate Auditor & Avail) for Preserving Integrity of Data in Cloud Computing

Cloud User

:: Files Information ::

CSP Name	File Name	Description	Request for Download
sss	test_8.txt	test	download

Fig. 7: Data owner request for DL

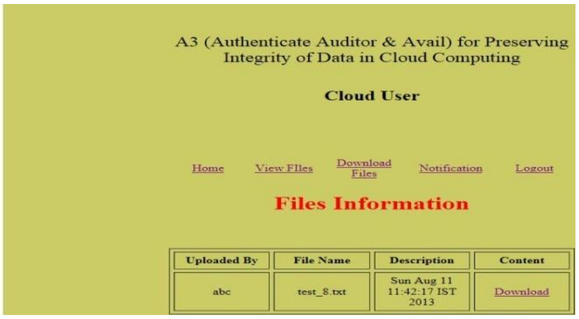


A3 (Authenticate Auditor & Avail) for Preserving Integrity of Data in Cloud Computing

Proof Information

CSP Name	File Name	Description	Proof
sss	test_8.txt	test	9d0bf03bf2b61e5f14fefb2157caa1d2

Fig. 8: TPA will grant DL after checking proof



A3 (Authenticate Auditor & Avail) for Preserving Integrity of Data in Cloud Computing

Cloud User

Files Information

Uploaded By	File Name	Description	Content
abc	test_8.txt	Sun Aug 11 11:42:17 IST 2013	Download

Fig. 9: Cloud user will DL file

6. Conclusion

The proposed system is suitable for providing integrity protection of customer data. The proposed system is proved to be secure against non-trusted server. It also secure from impersonate TPA. Both theoretical analysis and experimental results (simulation based) demonstrate that the proposed system has good efficiency.

Future Work

There are three main aspects to make the system robust and efficient 1.Data Integrity 2.Data Availability 3.User Authentication. The proposed system covers Data Integrity by using TPA and also checks whether TPA is valid or not. As a future work, we can make cloud more efficient by adding authentication and user privileges to the cloud user.

Reference

[1] Mertz S A, Eschinger C, Eid T, Pring B (2007) Dataquest Insight: SaaS Demand Set to Outpace Enterprise Application Software Market Growth.Gartner RAS core research Note 3 Aug. 2007.

[2] Right Scale (2008) Define Cloud Computing. RightScale Blog, 26 May 2008.

[3] Sun (2009a). A Guide to Getting to Started with Cloud Computing. Sun White paper.

[4] Jon Brodkin Gartner: Seven cloud computing security risks [EB/OL] 2009.

[5] Ling Li Lin Xu Jing Li Changchun Zhang "Study on the Third-party Audit in cloud storage service" IEEE 2011.

[6] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing" IEEE TRANSACTION ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL 22 NO 5 MAY 2011.

[7] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou "Security and Privacy in Cloud Computing: A Survey" IEEE 2010.

[8] Thorsten Holz, Markus Engelberth, Felix Freiling, "Learning More About the Underground Economy: A Case-Study of Keyloggrs and Dropzones", December 18, 2008. www.scribd.com/doc/9191346/Impersonation-Attacks-TR .

[9] IIA Chicago chapter 53rd Annual Seminar April 15, 2013, Donald E. Stephans Convention Center. On "Cloud Computing: Risks and Auditing" .

[10] C. Wang, K. Ren, W. Lou and J. Li. "Towards publicly auditable Secure Cloud data Storage Service" IEEE Network Magazine, vol. 24, no. 4, pp. 19-24 July/Aug 2010.

[11] M. A. Shah, M. Baker, J. C. Mogul and R. Swaminathan, "Auditing to keep online Storage Services Honest" Proc. 11th USENIX WORKSHOP HOT TOPICS IN OPERATING SYSTEM, pp. 1-6-2007.

[12] William Stalling "Cryptography and Network Security" Tata McGraw Hill Publication.

[13] Charlie Kaufman, Radia Perlman, Mike Speciner, "NETWORK SECURITY Private Communication in Public World" Pearson Education Publication.

Sagar Sawant has completed B.E. from Shivaji University Kolhapur, Pursuing M-Tech from JNTU, Hyderabad. He is working as a Asst. Professor in Rajarambapu Institute of Technology (An Autonomous Institute), Islampur, Sangli, and Maharashtra. The area of interest is Cloud Computing.

Suhit Kalubarme is pursuing B.E. from Rajarambapu Institute of Technology (An Autonomous Institute), Islampur, Sangli, and Maharashtra.