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. 8, August 2014, pg.219 – 229

RESEARCH ARTICLE

Auditing Mechanisms for Outsourced Cloud Storage

J.Aparna[1], Mr.R.Sathiyaraj[2]

[1]PG Student of CSE, Madanapalle Institute of Technology & Science, JNTUA University, A.P, India

[2]Assistant Professor, Department of CSE, Madanapalle Institute of Technology & Science, JNTU University, A.P, India

Aparna03.jogi@gmail.com sathiya.peace@gmail.com

Abstract- As we know that most of the firms are shown interested to place their data in a cloud based networks because of its utilities and problems with traditional data storage tools. If we are storing data outside of its environment means outsourced it leads to privacy issues. Also considerable factor is that security here users worried about integrity and accountability. Security is a considerable issue for this type of data centers. Security consist set of policies, applications and infrastructure. In this article we propose a model to overcome these issues; Outsourced data are verified by trusted third party persons to ensure its integrity. This auditing was done because most of the data are outsourced. Next focused on security and performance analysis issues this was done by auditors simultaneously without over burden to the users.

Keywords: Data storage, privacy-preserving, public audit ability, cryptographic protocols, cloud computing

I. INTRODUCTION

CLOUD computing have be envision like the next invention information technology (IT) structural design for enterprise, owing to its lengthy catalog of extraordinary compensation in the IT record: on demand identity service, everywhere system access, position self-governing resource pool, rapid store flexibility, usage based price and transfer of threat. The same as a troublemaking skill with thoughtful implication cloud computing is transform the incredibly character of how business use IT. Single elementary feature of this archetype changing is to information be organism regional before outsourced to the confuse storage. As of user point of view, together with mutual persons with IT enterprise, store information distantly to the cloud within a supple on order method bring interesting profits: release of the load for storage managing, entire information accessing by location self-determination, and prevention of resources expenses on hardware, software, and human resources maintenance, etc., whereas cloud compute make these compensation more interesting than ever, it as well bring new and demanding security pressure toward user outsourced information.

Ever since cloud service providers (CSP) are different organizational entities, data outsourcing is actually relinquish user's crucial manage over the destiny of their information.

The same as an outcome, the appropriateness of the information in the cloud is being put at possibility due to the next reason. Firstly, though the framework in the clouds is very much more great and consistent than individual compute procedure, they are immobile face the wide range of both external and internal pressure for information reliability. Example of outages and protection breach of notable cloud service come out from time up to date. Next, these do survive various motivation for cloud service provider to perform falsely toward the cloud user as regards their outsource information kind. For example, cloud service provider might retrieve storage space for economic reason by throwing away information that have not be or are infrequently access, or constant hides information lost incident to sustain a repute. In brief, though outsourced information to the cloud is inexpensively gorgeous for long term large scale storage, it doesn't instantly propose any assurance on data reliability and accessibility. That complexity, if not accurately address, may obstruct the success of cloud structural design.

Since users no longer actually acquire the storage of that information, conventional cryptographic primitive for the reason of information security defense can't be straight adopt. During exacting, basically downloads all the information for it's reliability authentication is not a useful solutions suitable to the expensiveness in Input Output and communication expenses across the system.

Further, that is continually inadequate to determine the information correctness only while accessing the information, as it does not gives user accurateness maintain for that unaccessed information and may be too overdue to recovering the data lost or damages. Assume the huge volume of the outsource information and the users confine source capacity, the responsibilities of audit the information correctness in a cloud location should be horrible and more costly for the cloud user. As well, in the clouds of usage of cloud storage space can be decrease as possible, for this a user doesn't require to do too many number of tasks to using the data. Specially, user might not to go throughout the difficulty in verify the data consistency. Additionally may be there more number of users access the similar cloud storage space, articulate in an activities settings. For easy managing, that is attractive this cloud only entertain authentication demand from a one preferred party.

By totally make sure the information reliability and saves the cloud user calculation resources also burden of online, that is of critical consequence to allow auditing mechanism for security storage in cloud, for this user may alternative to an self-determining Third Party Auditor (TPA) to auditing the outsourcing information where it needs. The T PA who have awareness and capacity these user don't, from time to time checking the reliability of all the information store into the cloud on half of the applicants, which provide a very easily and reasonable way for the users to make sure that storage accuracy into the clouds. In accumulation, to assist users to estimate the threat of their subscribe cloud information service, the auditing results from TPA should also be useful for the cloud services provider to improving that cloud base services proposal, and then provide for autonomous negotiation purposes. Here in a word, enable public auditable service will act as major responsibility for that hopeful cloud saving to develop into full established, where as a user will required ways to assessing risks and achieve hope in the clouds. In recent times, the opinion of public auditing have be anticipated into the perspective of ensure distantly store information reliability in dissimilar systems and security representations. Public auditing allow an outside parties, in accumulation to the users himself, to make sure the accuracy of distantly stores information. Although, a large amount of these scheme, don't considering the confidentiality security of user information against outside auditor. in fact, they are potentially make known user's information to auditors.

That cruel disadvantage significantly affects the protection of that protocol in cloud compute technique. From view of defensive information confidentiality, the applicants, who possess the information and rely on Third Party Auditor presently for the storage protection for that data, don't want that auditable procedure introduce latest damages of illegal data outflow towards that information protection. Here those are authorized system, such as the US (HIPAA) Health Insurance Portability and Accountability Act advance demands the outsourced information is not leaked to outside party. Simply exploiting information encryption prior to outsourcing could be single way to moderate that confidentiality concern of information auditing, other than it can also be an excess when in use in case of un encrypted/ public clouds information, appropriate to the preventable process load for the cloud user. In accumulation, encrypted technique doesn't totally solves the difficulties of protected information confidentiality beside third party auditable however immediately reduce it into the complexion key managing region.

Reasonable information leak at a standstill residue possible appropriate to the prospective coverage of decryption key. For that cause, how to make possible confidentiality preserve third party auditable procedure, autonomous to information encryption, is the trouble we are obtainable to attempt in this project. Our employment is with the primary the minority to sustain auditing mechanism for secure cloud storage, among important point on information storages. In adding together, with the occurrence of cloud compute, an anticipated enhance of auditable responsibilities commencing different user may be assign to Third Party Auditor. The same as the entity audit of these increasing responsibilities should be boring and unwieldy a usual command is then how to facilitate the Third Party Auditor to capably performing multiuser auditable responsibilities in a group manner, that is, at the same time.

To concerted on these troubles, In our project uses the procedures of public key base homomorphism linear authenticator. Which enable TPA to perform the auditing exclusive of challenging the confined copy of information and these considerably reduce the communications and calculation transparency as compare to the straight forward data auditable approach.

The aggregation and geometric property of the authorized user additional advantage our plan for the batch auditable process. Specially, our involvement can be summarizing as the follow three aspects:

1. Inspire the free auditable organization of information storage space protection in the cloud compute and providing a Auditing mechanism for secure cloud storage. Our method allows outside auditor to auditing the user cloud information without learn the information's contented.

2. For the most of our information, our method is the first to supporting scalable and capable auditable method for out sourced cloud storage space.

3. Here we express the protection and validate the performance of our anticipated scheme during concreted experiment and comparison with the time to time

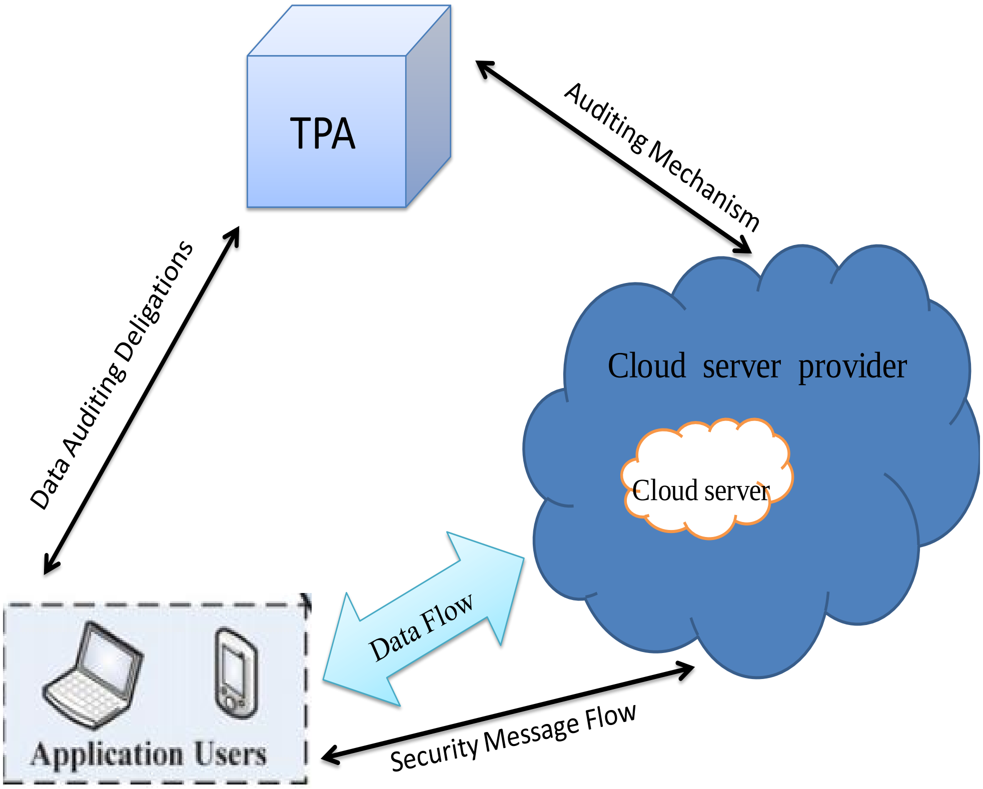
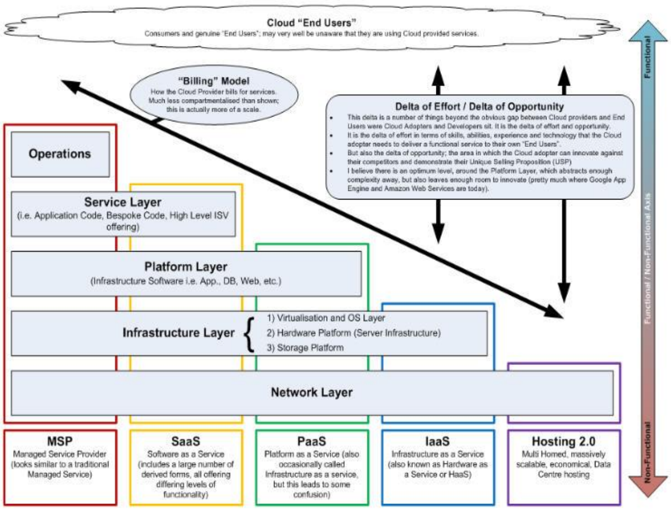
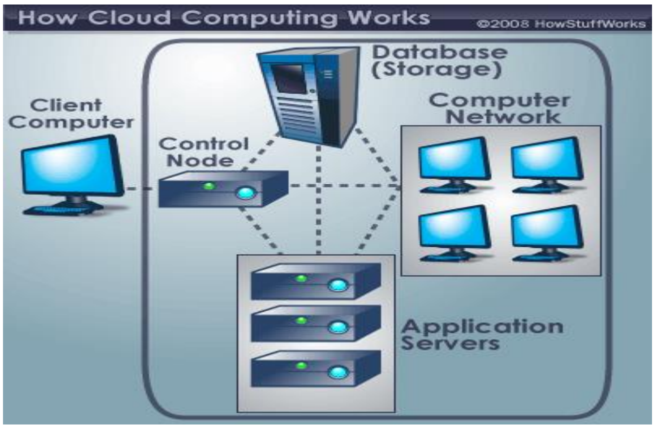


Fig. The Design of Auditing mechanism for outsourced cloud storage

II. RELATED WORK

Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, comprises hardware and software designed by a cloud architect who typically works for a cloud integrator. It typically involves multiple cloud other over application programming interfaces, usually web services.


Cloud "End Users"
Consumers and genuine "End Users"; may very well be unaware that they are using Cloud provided services.
"Billing" Model
How the Cloud Provider bills for services. Much less compartmentalised than shown; this is actually more of a scale.
Delta of Effort / Delta of Opportunity
This delta is a number of things beyond the obvious gap between Cloud providers and End Users were Cloud Adopters and Developers sit. It is the delta of effort and opportunity.
It is the delta of effort in terms of skills, abilities, experience and technology that the Cloud adopter needs to deliver a functional service to their own "End Users".
But also the delta of opportunity; the area in which the Cloud adopter can innovate against their competitors and demonstrate their Unique Selling Proposition (USP)
I believe there is an optimum level, around the Platform Layer, which abstracts enough complexity away, but also leaves enough room to innovate (pretty much where Google App Engine and Amazon Web Services are today).
Functional
Functional / Non-Functional Axis
Non-Functional
Operations
Service Layer
(i.e. Application Code, Bespoke Code, High Level ISV offering)
Platform Layer
(Infrastructure Software i.e. App., DB, Web, etc.)
Infrastructure Layer
1) Virtualisation and OS Layer
2) Hardware Platform (Server Infrastructure)
3) Storage Platform
Network Layer
MSP
Managed Service Provider (looks similar to a traditional Managed Service)
SaaS
Software as a Service (includes a large number of derived forms, all offering differing levels of functionality)
PaaS
Platform as a Service (also occasionally called Infrastructure as a service, but this leads to some confusion)
IaaS
Infrastructure as a Service (also known as Hardware as a Service or HaaS)
Hosting 2.0
Multi Homed, massively scalable, economical, Data Centre hosting



Cloud architecture extends to the client, where web browsers and/or software applications access cloud applications.

Cloud storage architecture is loosely coupled, where metadata operations are centralized enabling the data nodes to scale into the hundreds, each independently delivering data to applications or user.

A. Typical Cloud Computing System

Soon, there may be an choice for executive like you. Instead of install a group of software for each computer, you'd only have to load one application. That application would allow employees to log into a Web-based service which hosts all the programs the user would need for his or her job. Remote technology own by another company would run everything from e-mail to word processing to difficult data analysis programs. It's called **cloud computing**, and it could change the entire computer production. In a cloud computing system, there's an important workload shift. Local computers no longer have to do all the heavy exciting when it comes to running applications. The networks of computers that make up the cloud handle them instead. Hardware and software demands on the user's side reduce. The only thing the user's computer needs to be able to run is the cloud computing systems **interface software**, which can be as simple as a Web browser, and the cloud's network takes care of the rest.

There's a good chance you've previously used some form of cloud computing. If we have an e-mail account with a Web-based e-mail service like Hotmail, Yahoo! Mail or Gmail, then we've had some knowledge with cloud computing. Instead of running an e-mail program on our computer, we log in to a Web e-mail account remotely. The software and storage for our account doesn't exist on our computer – it's on the service's computer cloud.

B. What is Driving Cloud Computing

The CLOUD COMPUTING is driving in two Types of category.

Customer perspective

- In one word: economics
- Earlier, simpler, cheaper to use clouds compute
- No upfront capital required for servers and storage.
- No constant for ready expenses for running Data center.
- Application can be run from anywhere.

C. Vendor perspective

- Easier for request vendor to make new customers.
- Lowest cost way of deliver and supporting application.
- Ability to use product server and storage space hardware.
- Ability to drive down data center prepared costs.
- Computer hardware (Dell, HP, IBM, Sun Microsystems)
- Storages (Sun Microsystems, EMC, IBM)
- communications (Cisco Systems)
- Computer software's (3tera, Hadoop, IBM, RightScale)
- Operating systems (Solaris, AIX, Linux including Red Hat)
- proposal virtualization (Citrix, Microsofts, VMware, Sun xVM, IBM)

III. EXISTING METHODOLOGY

In the Existing method, the concept of public auditability has been anticipated in the framework of ensure distantly stored information reliability in special method and security model. Public auditability allows an outside gathering, in adding to the users himself to validate the accuracy of distantly stored information. Though, mainly of this scheme doesn't reflect on the confidentiality security of user data beside outside auditor. Certainly, they might potentially make public user data to auditor. Such cruel problem affects the protection of these protocol in cloud computing. since the point of view of protected data confidentiality, the user, who have the information and rely on TPA now for the storages protection of their data, don't desire this audit procedure introduce latest damages of illegal data leak to their information security.

Limitations Of Existing Method

Even though the infrastructures below the cloud are greatly further influential and consistent than individual computing procedure.

Encryption doesn't totally solve the difficulty of protective information confidentiality beside the third party auditor.

IV. PROPOSED METHODOLOGY

In this project, we use the public key base homomorphic authenticator and uniquely integrated. By this random mask techniques to attain an Auditing mechanism for outsourced cloud storage, whereas all above mentioned necessities in considerations. To sustain capable handle of several auditable responsibilities, In addition, we search the techniques of bilinear aggregation signatures to extend our major results into a multiple user's settings, wherever TPA can perform multi auditing responsibilities concurrently. Generally protection and presentation study shows the future schemes are provably make safe and highly efficiency. Here we also explain how to exposure our major schemes to support multiple tasks to TPA from delegation for batch auditing.

The following are the proposed methods that are used for Auditing mechanisms for outsourced cloud storage.

- Isolated information reliability examination protocol for cloud storages. The future scheme inherits the maintenance of information dynamics, and supports public verifiability and isolation beside third party verifiers, although at the same time it doesn't require to utilize a third party auditor.
- Protection study of the proposed systems, which showing with the aim of it is protected beside the untrusted server and confidential beside third party verifiers.

Advantages Of Proposed Method

1. Here we stimulate the public auditable scheme of information storage protection in cloud computing and make available a privacy preserving audit protocol. Our system enables exterior auditors to review user's cloud information devoid of knowledge the information contents.

2. The top of our information, our system is the initial to maintain scalable and able auditing mechanism for outsourced cloud storage. specially, our system achieve group audit where several delegate audit tasks from dissimilar user be able to be perform concurrently by the TPA in a privacy preserving approach.

3. Here confirm the protection and validate the show of our future scheme throughout existing experiment and comparison by the "state of the art".

To facilitate Auditing mechanism for outsourced cloud storage below the aforementioned models, our protocol design must accomplish the subsequent protection and presentation assurance:

1. Public audit ability: To consent to Third Party Auditor to authenticate the accuracy of the cloud information on demand without retrieve a replica of the entire information or introduce added on-line burden to the cloud users.

2. Storage correctness: To make sure that here exists no cheating cloud servers that can pass the check from Third Party Auditor without indeed store user's information intact.

3. Privacy preserving: To make sure that there exists no approach for Third Party Auditor to develop user's information contented from the information collect throughout the Auditing process.

4. Batch auditing: To allow Third Party Auditor with protected and capable auditing capacity to manage with various audit delegation as of probably great amount of dissimilar user concurrently.

5. Lightweight: To allow Third Party Auditor to perform audit with smallest amount communication and calculation overhead.

Algorithm

A public auditing scheme consists of four algorithms " KeyGen", "SigGen", "GenProof", and "Verify Proof ".

1. **KeyGen**: key generation algorithm that is run by the user to setup the scheme.

RSA involve a *public key* and a *private key*. The public key can be known by each one and is used for encrypting
Messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the
Private key. The keys for the RSA algorithm are generate the following way:
Step 1: Choose two distinct prime numbers p and q.
For security purpose, the integer p and q should be chosen at random, and should be of similar bit length.
Prime integers can be efficiently found using a primality test.
Step 2: Compute $n = pq$.
n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the
key length.

Step 3: Compute φ $(n) = φ(p)φ(q) = (p − 1)(q − 1) = n$ - $(p + q$ -1), where φ is Euler's totient function.
Step 4: Choose an digit e such that $1 < e < φ(n)$ and $\gcd(e, φ(n)) = 1$; i.e., e and $φ(n)$ are coprime.
e is release the public key example.
e have a short bit-length and small Hamming weight results in other efficient encryption – most
Generally 216 + 1 = 65,537. However, much smaller values of *e* (such as 3) have been shown to be
Less secure in various settings.

Step 5. Determine d as $d ≡ e−1$ (mod $φ(n)$); i.e., d is the multiplicative inverse of e (modulo $φ(n)$).

This is more clearly stated as: solve for d given $d⋅e ≡ 1$ (mod $φ(n)$)
This is frequently computed using the complete Euclidean algorithm. Using the pseudo code in the
Modular integers section, inputs *a* and *n* correspond to *e* and *φ(*n*)*, respectively.

1. *d* is kept as the private key exponent.
2. **SigGen**: used by the user to create confirmation metadata, this may consist of MAC, signatures or other information used for auditing.
3. **GenProof**: run by the cloud server to generate a proof of data storage correctness.
4. **Verify Proof**: run by the TPA to audit the proof from the cloud server**.**

V. IMPLEMENTATION

The segment of the project when the theoretical proposal is bowed out in to an operational scheme is said to be implementation. So it can regard as to be the most important segment in getting a gainful new scheme in give the operator, guarantee that the recent scheme will job and be competent.

The implementation step includes scheming of process to get different and estimation of different process, thoughtful setup, scrutiny of the accessible system and it’s limitation on carrying out.

1. Public Audit Ability For Storage Correctness Assurance

To assent to os, the operators who at first downloaded the folder on obscure server, to encircle the capability to confirm the exactness of the downloaded information is in sequence.

2. Operation Support Of Dynamic Data

To assent to the operators to carry out wedge stage process on the in order records whereas uphold the parallel level of in order exact assurance. The map must be as able as likely so as to make confident faultless combination shared audibility and energetic information practical support.

3. Block less Verification

The confront folder wedge mustn’t be recover in the verifier ex.TPA in support procedure used for efficacy distress.

4. Dynamic Data Operation with Integrity Assurance

In this demonstrate our system clearly with capably button completely energetic information procedure as well as information alteration (M), information inclusion (I) and information removal for obscure information storage space. In this message that in the successive descriptions, we superior to the folder F also the signature include previously be produce with suitably store in servers. Starting meta data R have been sign by operator with lay up into the obscure servers to others who have the user public key can demanding exactness of information storage space.

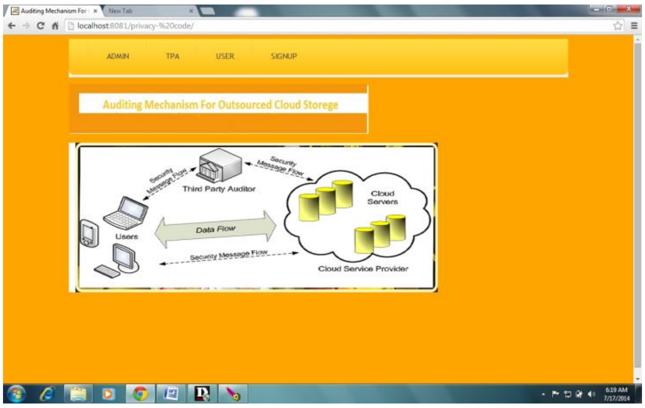
5. Data Modification

As we begin starting information changes, which is individual of biggest element commonly used operation in obscure information storages. The fundamental information variation procedure refers to the substitute of literal block with fresh ones. Starting base on the fresh block the user produce the similar signatures. The operators signs the fresh starting meta data R′ by sings (H (R′)) with throw it to server for renew. As a last point, the operator performing the problematic reliability authentication protocol. If the Output is CORRECT, cancel signs (H (R′)), and produce copied folders.

6. Batch Auditing for Multi-client Data

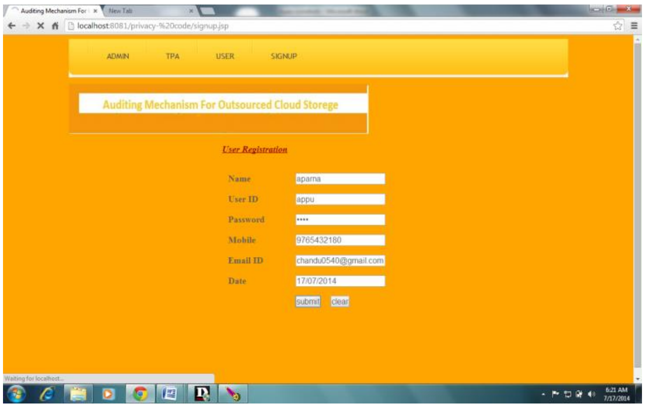
During obscure server may at the same time as grip many verification meetings from not equal operators, given K signature on K separate information folder starting K operator, it is extra beneficial to broad all these signature into a lonely small one with validate it one time. To getting this objective, we enlarge our system to allocate for confirmable information bring up to date and a validation in multi-client systems. The signature system allows the structure of signature on random various messages. In addition, it ropes the aggregation of several signature by not equal signers on dissimilar communication into an exact short signatures, and so appreciably decreases the statement value at the constant time as provided that competent validation for the exactness of all messages.

Home page



Auditing Mechanism For Outsourced Cloud Storege

User registration page



Auditing Mechanism For Outsourced Cloud Storege

User Registration

Name aparna

User ID appu

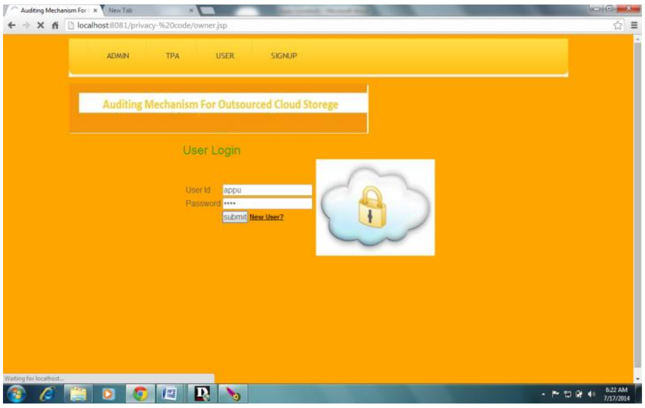
Password ••••

Mobile 9765432180

Email ID chandu0540@gmail.com

Date 17/07/2014

Login page



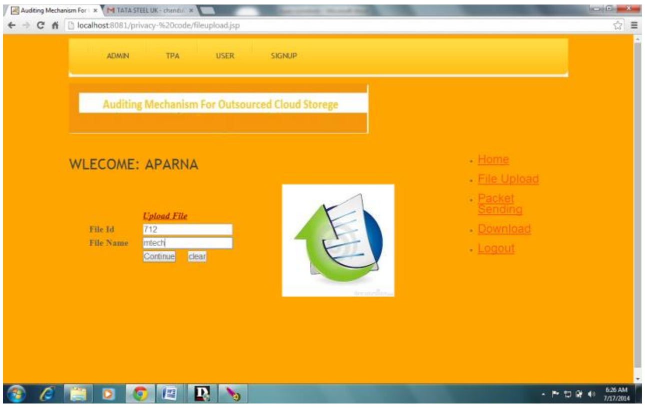
Auditing Mechanism For Outsourced Cloud Storege

User Login

User Id appu

Password ••••

File uploading page



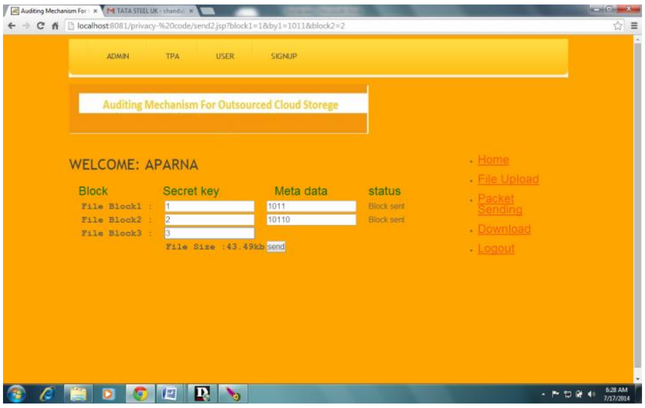
WLECOME: APARNA

Upload File

File Id 712

File Name mtech

Changing normal data into meta data

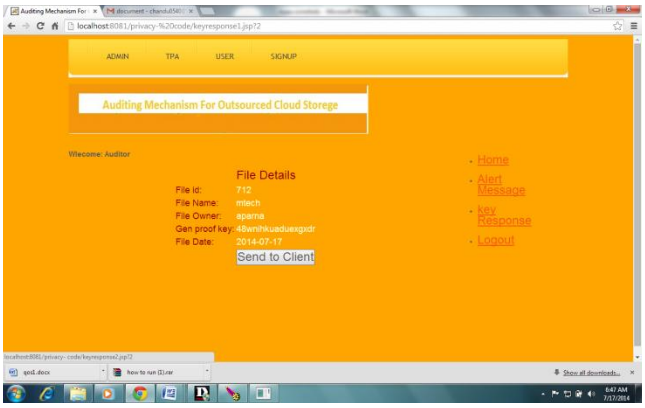


WELCOME: APARNA

Block	Secret key	Meta data	status
File Block1 :	1	1011	Block sent
File Block2 :	2	10110	Block sent
File Block3 :	3		

File Size :43.49kb

Data files sending to TPA page



Wlecome: Auditor

File Details

File id: 712

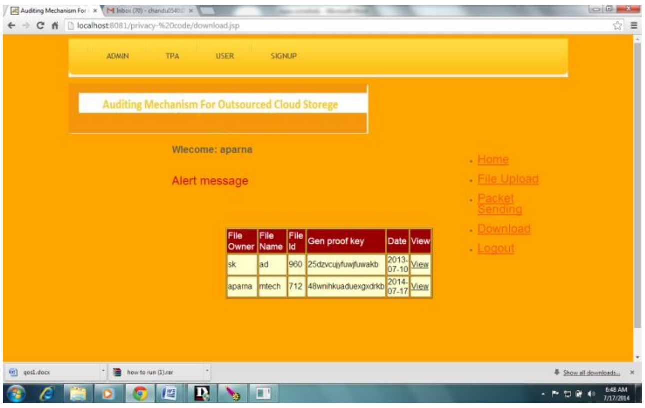
File Name: mtech

File Owner: aparna

Gen proof key: 48wnihkuaduexgxdr

File Date: 2014-07-17

File downloading page



Auditing Mechanism For Outsourced Cloud Storege

Wlecome: aparna

Alert message

- Home
- File Upload
- Packet Sending
- Download
- Logout

File Owner	File Name	File Id	Gen proof key	Date	View
sk	ad	960	25dzvcujyfuwjfuwakb	2013-07-10	View
aparna	mtech	712	48wnihkuaduexgxdrkb	2014-07-17	View

VI. ADVANCED ISSUES IN CLOUD COMPUTING SECURITY

In the prior segment, we contain discuses common set of safety concern useful in public and hybrid clouds. Currently circle our center to some a usual cloud exact security issues. In exact, cloud does find out a set of unique challenge like:

Concept: Cloud's provides a conceptual place of service end-point. For users, it is not possible to pin-point in which physical device, storage division (LUN), network port MAC address, switch etc. Actually complex. Thus, in event of security breach, it becomes difficult for a user to separate a particular physical store to have a threats or have be compromise.

Lack of execution control: The external cloud users do not contain fine-gained control more remote effecting location. Hence the critical issues like memory executive, Input calls, access to external public utilities and data are remote the preview of the user. Client would want to study the execution traces to ensure that illegal operation are not perform.

Third-party control of data: In clouds, the storage space communications, and thus, the data controls is also with the providers. So constant if the cloud's providers vouches for data confidentiality and integrity, the client may need verifiable proofs for the same.

Multi-party processing**:** In multi-clouds scenario, one party maybe use fraction of the data which further party provide. In lack of strong encryption (as data is individual process), it become essential for participate cloud computing party to protect privacy of individual data.

Data breach is a big concern in cloud computing. A compromise servers cloud's significantly harm the users as well as cloud provider. A selection of data could be real stolen. These contain credit card and social security numbers, address, and individual messages. The U.S. currently require cloud provider to report clients of breach. Once notify, clients now include to worry about identify theft and scheme. While provider, have to transaction with central investigation, lawsuit, and bad character. client lawsuit and settlement contain result in more $1 billions in victims to cloud provider Since users no longer actually acquire the storage of that information, conventional cryptographic primitive for the reason of information security defense can't be straight adopt. During exacting, basically downloads all the information for it's reliability authentication is not a useful solutions suitable to the expensiveness in Input Output and transmission expenditure across the system.

VII. CONCLUSION

Here we intend an Auditing mechanism for outsourced cloud storage. We make use of the homomorphism linear authenticator and random masking to assurance that the Third Party Auditor wouldn't study any information regarding the information content store on the cloud servers throughout the efficient audit procedure, which not only eliminate the load of cloud users from the tedious and perhaps exclusive auditable tasks, but also alleviate the users fear of their outsourced information outflow. Taking into consideration Third Party Auditor might at the same time as handling various auditing sessions from dissimilar clients for their outsourced information files, we additional expand our Auditing mechanism for outsourced cloud storage into multi user settings, where the Third Party Auditor can execute several audit tasks in a group approach for enhanced effectiveness. Wide-ranging study shows that our scheme is provably protected and extremely competent.

VIII. FUTURE WORK

We visualize more than a few possible instructions for prospect examine on this region. The mainly capable one we consider is a model in which public verifiability is enforced. Public verifiability, allow TPA to auditing the clouds information storage space without difficult user's time, possibility or funds. An attractive issue in this model is if we can make a system to realize mutually public verifiability and storage truth declaration of dynamic data. In adding, beside with our revise on dynamic cloud data storages, we can also plan to use Trapdoor Commitment system.

REFERENCES

[1] Privacy Preserving Public Auditing for Secure Clouds Storage Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, Kui Reno, Member, IEEE, and Wenjing Lou, Member, IEEE IEEE TRANSACTIONS ON CLOUD COMPUTING YEAR 2013

[2] Abraham, G. Chockler, I. Keidar and D. Malkhi, "Byzantine disk paxos: optimal resilience with Byzantine shared memory", Distributed Computing, 18(5), 2006, pp. 387-408.

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep.

[4] Kincaid, "MediaMax/TheLinkup Closes Its Doors," Online at mediamaxthelinkup-closes-its-doors/, July 2008.

[5] H. Abu-Libdeh, L. Princehouse and H.Weatherspoon, "RACS: a case for cloud storagediversity", SoCC'10:Proc. 1st ACM symposium onCloud computing, 2010, pp. 229-240.

[6] S. Wilson, "Appengine outage," Online .cio-weblog.com/50226711/appengine outage.php, June 2008.

[7] B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at 2009/01/payment processor breach may b.html, Jan. 2009.

[8] D. Agrawal, A. El Abbadi, F. Emekci and A.Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716.

[9] M.A. AlZain and E. Pardede, "Using Multi Shares for Ensuring Privacy in Database-as-a-Service", 44th Hawaii Intl. Conf. on System Sciences (HICSS), 2011, pp. 1-9.

[10] A. Bessani, M. Correia, B. Quaresma, F.André and P. Sousa, "DepSky: dependable and secure storage in a cloud-of-clouds", EuroSys'11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.