Ensuring Liability and Security in Cloud

Piyush Kumar Singh, Amit Kumar Choudhary, Ankit Kumar Singh

Abstract— Cloud 3)computing enables highly scalable services to be easily consumed over the internet on as need. In cloud computing services uses data is generally processed by online basis or remotely through unknown machines and unknown places. Due to this reason user or service provider is always in fear regarding data loss due to every day emerging new technologies. So ensuring data liability and security in cloud is very important . In this paper present a YAK 5) and encryption algorithm for data liability and security in cloud 6).

Index Terms— YAK 1), ELSC, Encryption algorithm 4), Access Control List 2), Cloud Services 7)

1 INTRODUCTION

CLOUD computing presents a brand new thanks to supplement this consumption and delivery model for IT services supported the web, by providing for dynamically climbable and infrequently virtualized resources as a service over the web. Users might not apprehend the machines that really method and host their knowledge. Whereas enjoying the convenience brought by this new technology, users conjointly begin worrying concerning losing management of their own knowledge. The info processed on clouds area unit typically outsourced, resulting in variety of problems associated with responsible-ness, as well as the handling of person specifiable info. Such fears have become a major barrier to the wide adoption of cloud services To allay users' issues, it\'s essential to supply an efficient mechanism for users to watch the usage of their knowledge within the cloud. For instance, users ought to be ready to make sure that their knowledge area unit handled consistent with the service level agreements created at the time they sign up for services within the cloud. Typical access management approaches developed for closed domains like databases and operative systems, or approaches employing a centralized server in distributed environments, aren't appropriate, thanks to the subsequent options characterizing cloud environments. First, knowledge handling will be outsourced by the direct cloud service supplier (CSP) to different entities within the cloud and theses entities may delegate the tasks to others, and so on. Second, entities area unit allowed to hitch and leave the cloud in an exceedingly versatile manner. As a result, knowledge handling within the cloud goes through a fancy and dynamic hierarchic service chain that doesn't exist in typical environments. To beat the higher than issues, we tend to propose a unique approach, particularly ELSC framework, supported the notion of knowledge responsible-ness . in contrast to privacy protection technologies that area unit designed on the hide-it-or-lose-it perspective, info responsible-ness focuses on keeping the info usage clear and track ready. Our projected ELSC framework provides finish-to end responsible-ness in an exceedingly extremely distributed fashion. One in all the most innovative options of the ELSC framework lies in its ability of maintaining lightweight weight and powerful responsible-ness that mixes aspects of access management, usage management and authentication. By suggests that of the ELSC, knowledge homeowners will track not solely whether or not or not the service-level agreements area unit being honored, however conjointly enforce access and usage management rules as required. We tend to conjointly develop two distinct modes for auditing: Offset mode and Onset mode. The onset mode refers to logs being sporadically sent to the info owner or neutral whereas the offset mode refers to another approach whereby the user (or another licensed party) will retrieve the logs as required. the look of the ELSC framework presents substantial challenges, as well as unambiguously distinctive CSPs, making certain the responsible-ness of the log, adapting to a extremely localized infrastructure, etc.

2 RELATED WORK

2.1 Cloud Services

Software as a Service (SaaS) 10) : The potential provided to the buyer is to use the provider's applications running on a cloud infrastructure. The applications area unit accessible from numerous consumer devices through either a skinny consumer interface, like an internet browser (e.g., web-based email), or a program interface. the buyer doesn't manage or management the underlying cloud infrastructure as well as network, servers, in operation systems, storage, or maybe individual application capabilities, with the doable exception of restricted user-specific application configuration settings .

Platform as a Service (PaaS): The potential provided to the buyer is to deploy onto the cloud infrastructure consumer-created or non heritable applications created exploitation programming languages, libraries, services, and tools supported by the supplier. The buyer doesn't manage or management the underlying cloud infrastructure as well as network, servers, in operation systems, or storage, however has management over the deployed applications and presumably configuration settings for the application-hosting setting .

Infrastructure as a Service (IaaS): The potential provided to the buyer is to provision process, storage, networks, and different basic computing resources wherever the buyer is in a position to deploy and run discretionary code, which might embrace in operation systems and applications. The buyer doesn't manage or management the underlying cloud infrastructure however has management over in operation systems, storage, and deployed applications; and presumably restricted management of choose networking elements (e.g., host firewalls)

3 CLOUD ACTOR IN ELSC MODEL:

1. Information owner : Entity which will authorize or deny access to sure information, and is chargeable for its accuracy, integrity, and timeliness is thought as information owner. Information house owners ought to be creating selections regarding UN agency gets access to their information and its correct use of it.
2. Stakeholders: Person, cluster or Organization that has interest or concern in a company. Stakeholders will have an effect on or be littered with the organization\'s actions, objectives and policies. Some samples of key stakeholders area unit creditors, directors, employees, government (and its agencies), house owners (shareholders), suppliers, unions, and also the community from that the business attracts its resources.
3. Users: End-user, a final user of a poster product or sevice.

4 ISSUES IN CLOUD SECURITY: ICA TRIAD (INTEGRITY, CONFIDENTIALITY, AVAILABILITY)

Integrity: Integrity refers to data that has not been modified in associate degree unauthorized manner or by associate degree unauthorized person.

Confidentiality: Confidentiality may be a set of rules or a promise that limits access or places restrictions on sure kinds of data.

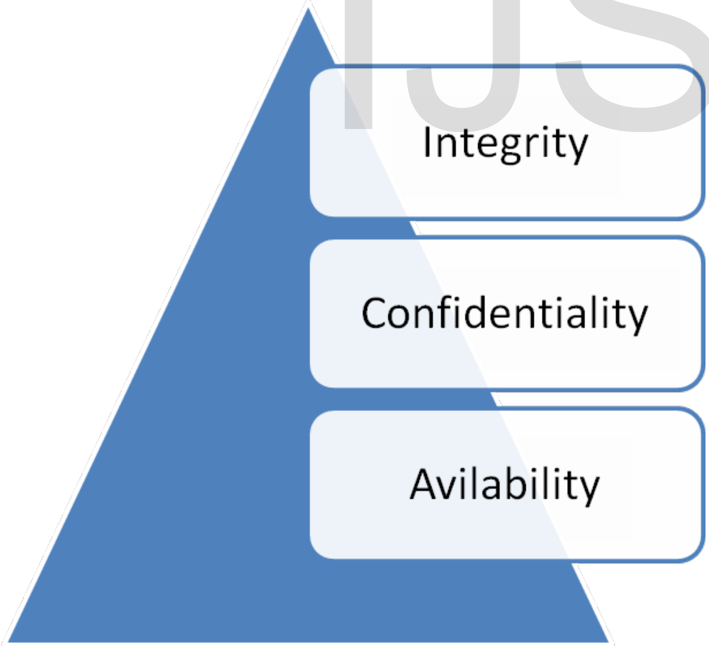


Figure 1: ICA Triad

Availability: Convenience of a system may additionally be exagge rated by the strategy on that specialize in increasing testability & maintainability and not on dependability. Up maintainability is mostly easier than dependability.

5 PROBLEM STATEMENT:

We begin this section by considering associate degree illustrative example that is the idea of our downside statement and can be used throughout the paper to demonstrate the most options of our system.
Example 1. Abhi, a book publisher and author, plans to sell his by exploitation the Cloud Services. For her business within the cloud, she has the subsequent requirements:

1. His books area downloaded solely by users who have procured her services.
2. Potential patrons area allowed to look at his book initial before they create the payment to get the transfer right.
3. Owing to the character of a number of his works, solely users from sure countries will read or transfer some sets of chapters
4. For a few of his works, users area allowed to solely read them for a restricted time, in order that the users cannot reproduce her work simply.
5. Just in case any dispute arises with a consumer, he needs to possess all the access data of that consumer.
6. She needs to confirm that the cloud service suppliers don\'t share his information with different service suppliers, in order that the responsible-ness provided for individual users may also be expected from the cloud service suppliers.

With the on top of state of affairs in mind, we have a tendency to determine the common necessities and develop many pointers to realize information responsible-ness within the cloud. A user signed to a particular cloud service, sometimes must send his/her information further as associated access management policies (if any) to the service supplier. When the information area received by the cloud service supplier, the service supplier can have granted access rights, like scan, write, and copy, on the information. Exploitation typical access management mechanisms, once the access rights area granted, the information are totally on the market at the service supplier.

Ensuring distributed responsible-ness for information sharing within the cloud information, we have a tendency to aim to develop novel work and auditing techniques that satisfy the subsequent requirements:

1. The work ought to be suburbanized so as to adapt to the dynamic nature of the cloud. A lot of specifically, log files ought to be tightly finite with the corresponding information being controlled, and need bottom infrastructural support from any server.
2. Each access to the user’s information ought to be properly and mechanically logged. This needs integrated techniques to certify the entity that accesses the information, verify, and record the particular operations on the information further because the time that the information are accessed.
3. Log files ought to be reliable and tamper proof to

avoid dirty insertion, deletion, and modification by malicious parties. Recovery mechanisms are fascinating to revive broken log files caused by technical issues.

4. Log files ought to be sent back to their information house owners sporadically to tell them of this usage of their information. a lot of significantly, log files ought to be recoverable anytime by their information house owners once required regardless the placement wherever the files area unit keep.
5. The planned technique shouldn\'t intrusively monitor information recipients' systems, nor it ought to introduce significant communication and computation overhead, that otherwise can hinder its practicableness and adoption in observe.

6 Proposed System:

6.1 Encryption Algorthim

6.2 Security Measures

6.1 Encryption Algorthim

6.1.1 CONNECTION ESTABLISHMENT:

1) Once the user initial involves cloud server. Cloud server provides him type to understand his essential details.
2) User forwards the crammed type to the cloud server for his account creation.
3) The affiliation institution by YAK protocol.
4) The server generates a novel ID and its corresponding key.
5) The server forwards the distinctive ID to the user.
6) The key generated adore user id area unit keep in a very key repository and forwarded to the information owner.

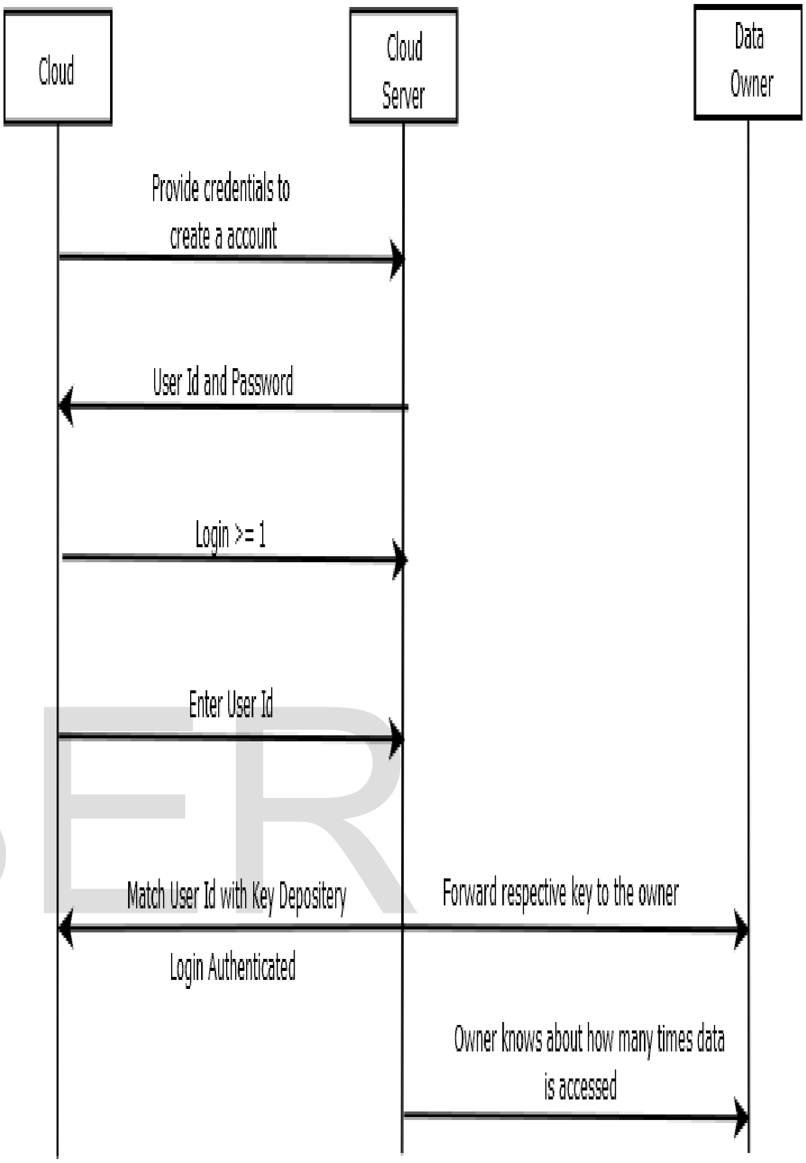
6.1.2 USER AUTHANTICATION AND KEY GENERATION

1) Once the user login next time is uses its user id for the authentication functions.
2) User forwards its user id to the cloud server.
3) Cloud server matches its user id with the corresponding YAK key that is generated at the time of affiliation institution and keep within the key repository.
4) Once the user is login a table is forwarded to the owner that contains YAK key, no of your time key accessed, date and time.
5) This table provides the owner that his information is accessed what quantity no of times over a period of time or perioadically.

6.2 Security Measures:

TABLE1
CLOUD ACTOR VS ACCSESS CONTROL

Actor/Access Controls	Access	Process	Store
Cloud Owner	✓	✓	✓
Stake Holder	✓	✓	
Users	✓		


Cloud
Cloud Server
Data Owner
Provide credentials to create a account
User Id and Password
Login >= 1
Enter User Id
Match User Id with Key Depositery
Forward respective key to the owner
Login Authenticated
Owner knows about how many times data is accessed

. Figure 2: Table Forwarding Procedure

As per security measures cloud owner can Access, Process and Store data over cloud ,stake holder only can Access and Process data over cloud ,wherever there is a limited permission for users. User can only access data on cloud .

Cloud computing is a vital scope for service delivery model .Over cloud there is a unlimited data which is crucial an important in many aspects .So security is a measure concern in the cloud .For insuring liability over the cloud with providing high speed huge data availability, it is important to impose many kind of security measures .By these kind of liability and security concern there must be some permission oriented Actor and Access control. So there is limited access process and storage phenomena over the cloud .As per table this access , process and storage phenomena is discussed for Actor and Access control .

7 CONCLUSION:

Cloud computing 9) change the face of grid computing over the data and security issues .cloud can manage a huge amount of data over virtual world .Labiality and security are the measure concern over the cloud . This paper process cloud security algorithm using YAK protocol .YAK symmetric algorithm provide fast and secure accessibility of a data over the cloud. It saves user s from Man In Middle Attack(MIMA).. Cloud computing is a future of inherit resource utilization over the network. So proposed ELSC model 8) which is based on Yak protocol is an attempt for providing liability and ensuring security and this will the strong pillar for the future for providing security over various Attacks.Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. Authors are strongly encouraged not to call out multiple figures or tables in the conclusion—these should be referenced in the body of the paper.

REFERENCES

[1] Ankit Kumar Singh, Saroj Kumar, Abhishek Rai “Secure Cloud Architecture Based on YAK and ECC” International Journal of Computer Applications(0975-8887)Volume 90-NO.19,March 2014.

[2] Ruj S, Nayak A, Stomernovic I. DACC: distributed access control in clouds. 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11,IEEE Computer Society, 2011:91-98.

[3] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. “What’s Inside the Cloud? An Architectural Map of the Cloud Landscape.” IEEE Xplore,pp23-31,june.2009.

[4] S. Kamara and K. Lauter. Cryptographic cloud storage. In Financial Cryptography and Data Security (FC’10),volume 6054 of LNCS, pages136{149. Springer,2010.

[5] F.Hao.”ON ROBUST KEY AGREEMENT BASED ON PUBLIC KEY AUTHENTICATION” Proceedings of the 14th International Conference on Financial Cryptography and Data Security, Tenerife,Spain,LNCS6052,pp.383-390,Jan 2010.

[6] M.Joshi, YS Moudgil “SECURE CLOUD STOARGE” International Journal of Computer Science 2011, ijcscn.com.

[7] Yaoxue Zhang and Yuezhi Zhou_ “Transparent Computing: Spatio-Temporal Extension on von Neumann Architecture for Cloud Services” *TSINGHUA SCIENCE AND TECHNOLOGY, ISSN 1007-0214l l02/12l lpp10-21* Volume 18, Number 1, February 2013.

[8] Linlin Wu and Rajkumar Buyya “Service Level Agreement (SLA) in Utility Computing Systems” Cloud Computing and Distributed Systems (CLOUDS) Laboratory Department of Computer Science and Software Engineering The University of Melbourne, Australia.

[9] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem “A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture” *(IJACSA) International Journal of Advanced Computer Science and Applications,*Vol. 3, No. 10, 2012.

[10] https://cloudsecurityalliance.org/research/secaas/.