ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 5, November 2014

Security in Cloud by Diffie Hellman Protocol

Abdul Muttalib Khan, Mohd. Haroon Khan, Dr. Shish Ahmad

Abstract— Cloud computing permits extremely scalable services to be simply consumed over the net on as need. In cloud computing services uses information is usually processed by on-line basis or remotely through unknown machines and unknown places, because of this reason user or service supplier is often in worry relating to information loss attributable to each day emerging new technologies. Therefore guaranteeing information liability and security in cloud is incredibly necessary, during this paper gift a Diffie Hellman and coding rule for information liability and security in cloud's.

***Index Terms*—Cloud computing; ESLC; Diffe Hellman; ICA traid; Security Measures.**

I. INTRODUCTION

CLOUD computing presents [3] a spanking new due to sup-plement this consumption and delivery model for IT ser-vices supported the online, by providing for dynamically climbable and sometimes virtualized resources as a service over the online. Users may not apprehend the machines that actually methodology and host their data. Whereas enjoying the convenience brought by this new technology, users con-jointly begin worrying regarding losing management of their own data. The information processed on clouds area unit usually outsourced, leading to kind of issues related to responsible-ness, moreover yet handling of person identifiable data. Such fears became a serious barrier to the wide adoption of cloud services to allay users' problems, it\'s essential to provide an efficient mechanism for users to observe the usage of their data inside the cloud. As an example, users need to be able to check that that their area unit square measure handled in step with the service level agreements created at the time they sign in for services inside the cloud. Typical access management approaches developed for closed domains like databases and operative systems, or approaches using a centralized server in distributed environments, aren't acceptable, because of the following choices characterizing cloud environments. First, [2] information handlings are outsourced by the direct cloud service provider (CSP) to totally different entities at intervals the cloud and theses entities could delegate the tasks to others, and so on. Second, entities area unit allowed hitching and leaving the cloud in an extremely versatile manner. As a result, data handling inside the cloud goes through a elaborate and dynamic gradable service chain that doesn't exist in typical environments. To beat the upper than issues, we have a tendency to tend to propose a singular approach, significantly ESLC framework, supported the notion of information responsible-ness. In distinction to[7] privacy protection technologies that area unit designed on the hide-it-or-lose-it perspective, data responsible-ness focuses on keeping the information usage clear and track prepared. Our projected ESLC framework provides finish-to finish responsible-ness in a passing extraordinarily distributed fashion. One altogether the most innovative choices of the ESLC framework lies in its ability of maintaining light-weight weight and powerful responsible-ness that mixes aspects of access management, usage management and authentication. By suggests that of the ESLC, data owners can track not only whether or not or not the service-level agreements area unit being honored, but collectively enforce access and usage management rules as needed. We have a tendency to tend to jointly develop 2 distinct modes for auditing: Offset mode and Onset mode. The onset mode refers to logs being periodically sent to the information owner or neutral whereas the offset mode refers to a different approach whereby the user (or another authorized party) can retrieve the logs as needed. The design of the ESLC framework presents substantial challenges, additionally as unambiguously distinctive CSPs, ensuring the responsible-ness of the log, adapting to a much localized infrastructure, etc.

.

II. RELATED WORK

2.1 Cloud Services

A. Software as a Service (SaaS) :

The potential provided to the[5] customer is to use the provider's applications running on a cloud infrastructure. The applications area unit accessible from various shopper devices through either a thin shopper interface, like a web browser (e.g., web-based email), or a program interface. the customer doesn't manage or management the underlying cloud infrastructure moreover as network, servers, operative systems, storage, or even individual application capabilities, with the achievable exception of restricted user-specific application configuration settings .

B. Platform as a Service (PaaS):

The potential provided to the customer is to deploy onto the cloud infrastructure consumer-created or non transmissible applications created exploitation programming languages, libraries, services, and tools supported by the provider. the customer doesn't manage or management the underlying cloud infrastructure moreover as network, servers, operative systems, or storage, but has management over the deployed applications and presumptively configuration settings for the application-hosting setting .

C. Infrastructure as a Service (IaaS):

The potential provided to the customer is to provision method, storage, networks, and different basic computing resources where the customer is in an exceedingly position to deploy and run discretionary code, which could embrace operative systems and applications. The customer doesn't manage or management the underlying cloud infra-structure

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 5, November 2014

but has management over operative systems, storage, and deployed applications; and presumptively restricted management of select networking parts (e.g., host firewalls)

III. CLOUD ACTORS IN ESLC MODEL

A. Data owner :

Entity which [6] can authorize or deny access to positive info, and is liable for its accuracy, integrity, and timeliness is assumed as info owner. Information householders got to be making alternatives relating to an agency gets access to their information and its correct use of it.

B. Cloud service consumer/ provider:

Person, cluster or Organization that has interest or concern in an exceedingly company. Cloud service consumer/ provider can have a control on or be full of the organization's actions, objectives and policies. Some samples of key stakeholders area unit creditors, directors, employees, government (and its agencies), householders (shareholders), suppliers, unions, and additionally the community from that the business attracts its resources.

C. Cloud service consumer:

End-user, a final user of an advert product or service.

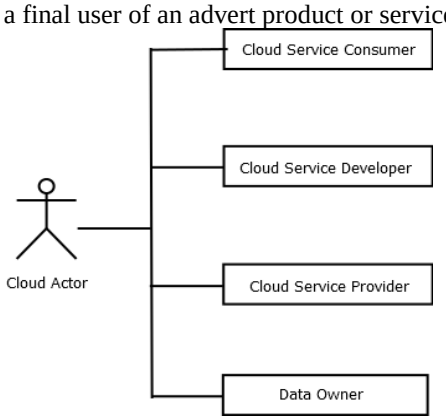

Fig 1- Cloud Actor

IV. ISSUES IN CLOUD SECURITY: ICA

TRIAD (INTEGRITY, CONFIDENTIALITY, AUTHENTICATION)

A. Integrity:

Integrity [1] refers to information that has not been changed in an unauthorized manner or by degree unauthorized person.

B. Confidentiality:

Confidentiality is also a group of rules or a promise that limits access or places restrictions on positive sorts of information.

C. Availability:

Convenience of a system could in addition be exaggerated by the strategy on it specialize in increasing testability & maintainability and not on responsibility. Up maintainability is generally easier than responsibility.

Fig 2: ICA

IV. PROBLEM STATEMENT

We begin this section by considering degree illustrative example that's the thought of our draw back statement and might be used throughout the paper to demonstrate the foremost choices of our system. Example- Abhi, a song publisher and author, plans to sell his by exploitation the Cloud Services. For her business at intervals the cloud, she has the next requirements:

1. His songs lyrics downloaded only by users who have procured her services.
2. Potential patrons lyrics allowed to seem at his song initial before they produce the payment to urge the transfer right.
3. Due to the character of variety of his works, only users from certain countries can browse or transfer some sets of songs.
4. For a couple of of his works, users lyrics allowed to only browse them for a restricted time, so as that the users cannot reproduce her work merely.
5. Simply just in case any dispute arises with a client, he must possess all the access information of that client.
6. She has to make sure that the cloud service suppliers don\'t share his info with totally different service suppliers, so as that the responsible-ness provided for individual users may additionally be expected from the cloud service suppliers.

With the on high of state of affairs in mind, we've got a bent to work out the common wants and develop several tips that could understand info responsibleness at intervals the cloud. A user signed to a specific cloud service, generally should send his/her information any as associated access management policies (if any) to the service provider. Once the knowledge lyrics received by the cloud service provider, the service provider will have granted access rights, like scan, write, and copy, on the knowledge. Exploitation typical access management mechanisms, once the access rights lyrics granted, the knowledge is wholly on the market at the service provider. Ensuring distributed responsible-ness for info sharing among the cloud info, we've got an inclination to aim to develop novel work and auditing techniques that satisfy the next requirements:

1. The work got to be decentralized therefore on adapt to the dynamic nature of the cloud. lots of specifically, log files got to be tightly finite with the corresponding info being controlled, and want bottom infrastructural support from any server.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 5, November 2014

2. Every access to the user's info got to be properly and automatically logged. This wants integrated techniques to certify the entity that accesses the data, verify, and record the actual operations on the knowledge additional as a result of the time that the knowledge are accessed.
3. Log files got 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 problems.
4. Log files got to be sent back to their info householders periodically to inform them of this usage of their information. Lots of considerably, log files got to be recoverable anytime by their info householders once needed regardless the position where the files square measure keeps.
5. The planned technique shouldn't intrusively monitor info recipients' systems, nor it got to introduce important communication and computation overhead, that otherwise will hinder its usefulness and adoption in observe.

V. PROPOSED SYSTEM

A. Encryption Algorithm

Once the user initial involves cloud server. Cloud server provides him kind to know his essential details. User forwards the crammed kind to the cloud server for his account creation. The affiliation establishment by DIFFIE HELLMAN protocol. The server generates a unique ID and its corresponding key. The server forwards the distinctive ID to the user. The key generated love user id area units confine a awfully key repository and forwarded to the information owner.

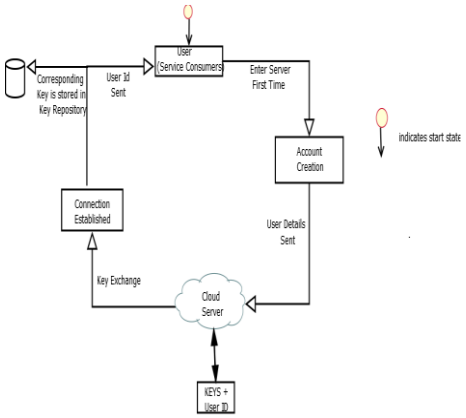

Fig 3- Proposed Encryption Algorithm

B. User Authentication and Key Generation

Once the user login next time is uses its user id for the authentication functions. User forwards its user id to the cloud server. Cloud servers matches its user id with the corresponding DIFFE HELLMAN key that's generated at the time of affiliation establishment and keep at intervals the key repository. Once the user is login a table is forwarded to the owner that contains DIFFE HELLMAN key, number of time key accessed, date and time. This table provides the owner that his info is accessed what amount no of your times over a amount of time or periodically.

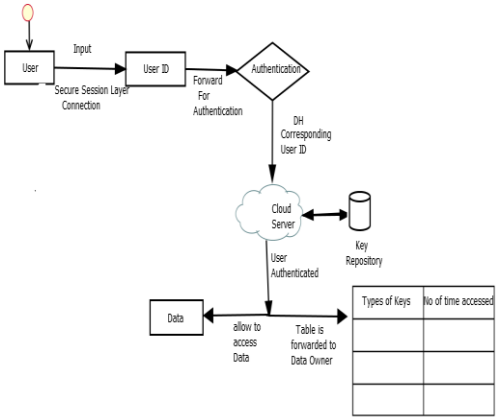

Fig 4: DH - Encryption Algorithm

C.Security Measures

TABLE 1 - CLOUD ACTOR VS ACCSESS management

Access Control/ Actor	Cloud service consumer	Cloud service developer	Cloud service provider	Data owner
Access	✓	✓	✓	✓
Process		✓	✓	✓
Store				✓

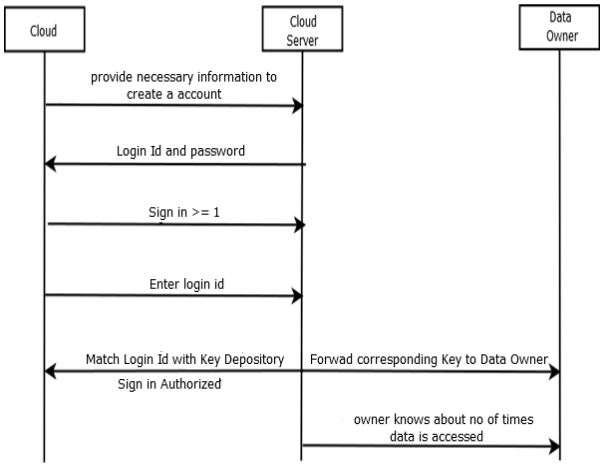

Fig 5: Sequence Diagram – Cloud, Cloud Server and Data Owner

As per security measures cloud owner will Access, method and Store information over cloud stake holder solely will Access and method information over cloud, wherever there's a restricted permission for users. User will solely access information on cloud. Cloud computing could be a important scope for service delivery model .Over cloud there's a unlimited information that is crucial a vital in several aspects .So security could be a live concern within the cloud .For insuring liability over the cloud with providing high speed and access to information handiness, it's vital to impose several reasonably security measures .By these reasonably liability and security concern there should be some permission

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 5, November 2014

homeward-bound Actor and Access management. Therefore there's restricted access method and storage phenomena over the cloud .As per table this access, method and storage phenomena is mentioned for Actor and Access management.

VI. CONCLUSION

Security issues are a major problems faced by the cloud computing paradigm. This paper focuses on how one can overcome the security issue faced by the data owner using diffie Hellman protocol. It basically tries to eliminate the insecurity faced by the data owner for his data is on cloud and under the control of the cloud provider. A secure channel is provided with the help of Diffie Hellman protocol such that no one except the data owner can access the data without his permission. Cloud computing has great and immense scope. Triple data scheme of encryption can be considered for maintaining security and liability of the data. Homomorphic encryption seems to be very effective but needs further study and consideration.

REFERENCES

[1] Ruj S, NaDiffe Hellman A, Stomernovic I. DACC: distributed access management in clouds. 2011 International Joint Conference of IEEE TrustCom-11/IEEE ICESS-11/FCST-11, IEEE pc Society, 2011:91-98.

[2] M. Klems, A. Lenk, J. Nimis, T. Sandholm and S. Tai. “What’s within the Cloud? Associate in nursing subject area Map of the Cloud Landscape.” IEEE Xplore, pp23-31, june.2009.

[3] S. Kamara and K. Lauter. Scientific discipline cloud storage. In money Cryptography and information Security (FC’10),volume 6054 of LNCS, pages136strong KEY AGREEMENT supported PUBLIC KEY AUTHENTICATION” Proceedings of the fourteenth International Conference on money Cryptography and information Security, Tene-rife,Spain,LNCS6052,pp.383-390,Jan 2010.

[4] M.Joshi, YS Moudgil “SECURE CLOUD STOARGE” International Journal of applied science 2011, ijcscn.com.

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

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

[7] Kawser Wazed Nafi, Tonny Shekha Kar, Sayed Anisul Hoque, Dr. M. M. A Hashem “A Newer User Authentication, File coding and Distributed Server based mostly Cloud Computing security architecture” (IJACSA) International Journal of Advanced applied science and Applications,Vol. 3, No. 10, 2012.

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