© 2018 IJSRSET | Volume 4 | Issue 7 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

An approach for Privacy Preserving of Encrypted Outsourced Data using Secret Key Distribution on Cloud

Pooja Arudkar, Prof. Vikrant Chole

Department of Computer Science & Engineering, G.H. Raisoni Academy of Engg & Technology, Nagpur, Maharashtra, India

ABSTRACT

Cloud computing has grow to be a trend with the supply of innumerable benefits. Cloud has end up an emerging well known that brings approximately diverse technology and computing thoughts for internet at very low fee. Huge storage centres are provided by the cloud which can be accessed without difficulty from any corner of the sector and at any time but there are sure problems and demanding situations confronted via the user whilst the use of cloud computing with regard to protection. But new demanding situations popped out to ensure Confidentiality, integrity and access manage of the information. To cope with those issues we will be predisposed to advise a subject matter that uses threshold cryptography inside which records proprietor divides customers in businesses and offers single key to every group in the mean time, that single key (separate via method that will become special mystery key) is distribute to every consumer of that cluster for decoding of records. The most feature of this subject is that cut again the number of safety key and it additionally make certain that entirely attested users can get entry to the outsourced know-how.

Keywords : Cloud Computing, Threshold Cryptography, Access Control, Authentication, Outsourced Data.

I. INTRODUCTION

Cloud computing is a growing computing paradigm inside which sources of the computing infrastructure are provided as offerings over the internet. Data security and access management is one in every of the most tough on-going evaluation works in cloud computing due to customers outsourcing their personal data to cloud providers.

Cloud computing growing as a latest paradigm for these days era inside the area of engineering and information technology. It is their enticing offerings like simple to use, on-line, on demand and pay as use scheme; it is past any doubt useful for tiny and big scale corporations due to it provide offerings at extraordinarily low charge. Cloud might be enterprise fashions which might be the one call for services to the user. Consumer will access those offerings any time at wherever inside the international. Demand of a cloud person cannot be foreseen due to the fact it can modification dynamically on runtime.

A cloud makes it possible to get right of entry to data from anywhere within the global at every time supplied internet connection must be available. It's far a type of parallel and allotted device which includes a group of interconnected and virtualized computers which might be dynamically provisioned and represented as one or greater unified computing sources based totally on provider degree agreements installed through negotiation between the service companies and purchasers. There are one-of-a-kind styles of cloud depending on wishes. This consists of personal cloud, public cloud, community cloud and hybrid cloud. public cloud may be accessed using net connection by way of any subscriber. Google and Microsoft offer public cloud. A private cloud is build

for unique organization or employer with gets right of entry to restrained to that institution. Community cloud is shared among corporation with comparable cloud necessities. Hybrid cloud is a aggregate of as a minimum any of cloud kind.

Cloud support three forms of offerings i.e. package as a Services (SaaS), Platform as a Services (PaaS) and Infrastructure as a Services (IaaS). it will be deployed in 3 completely exceptional method i.e. private cloud, public cloud and hybrid cloud non-public cloud is safer than the majority cloud.

IaaS clouds, example Amazon, offer virtualized hardware and storage in which the users can install their personal applications and offerings. PaaS clouds, like Microsoft azure, gives a software development environment for customers who assist them to put in force and run applications at the cloud. In accordance SaaS cloud there are two sorts of cloud, which provides software programs to the users. The primary organization gives the whole software as a provider to the end users that are used without any changes or customization. Examples of those styles of clouds are Google office automation carrier, like Google Document or Google calendar. The second one group affords on-demand for internet offerings to the Users, which may be used to construct more complex applications.

In brand new cryptography, most schemes are developed for a situation with one sender and one receiver. however, there are eventualities for the duration of which numerous receivers (or numerous senders) ought to be compelled to percentage the ability to use a cryptosystem the most motivation for threshold cryptography changed into to increase strategies to regulate the multi-sender/multi-receiver eventualities.

Many schemes are given to affirm these protection requirements but they're complete of collusion assault of malicious users and cloud provider supplier and extensive computation (because of massive no keys). To deal with these problems a topic is advocate, at some stage in this subject there square degree basically 3 entities: Data Owner (DO), Cloud service provider (CSP) and Users. Users square measure divided in groups on a few foundation like region, challenge, department and corresponding to each organization, there may be one key for encoding and deciphering of data. Data will be decrypted as soon as at the very least threshold range of users can present.

II. LITERATURE REVIEW

Information safety is a prime impediment inside the manner of cloud computing. Humans are nevertheless fearing to exploit the cloud computing. A few human beings consider that cloud is dangerous vicinity and once you ship your information to the cloud, you lose whole manipulate over it. A method which gives protection for facts outsourced at Csp. A few methods are given to comfortable outsourced data however they're suffering from having massive quantity of keys and collusion attack. by means of applying the edge cryptography at the user side, it is able to protect outsourced records from collusion assault and also provide authenticity of users.

Sushil kr saroj, et.al, has posted a research paper “threshold cryptography based totally information protection in cloud computing” [1].on this paper, a brand new method proposed which presents protection for information outsourced at Csp. some strategies are given to at ease outsourced understanding however they are stricken by having large quantity of keys and collusion assault. Through using the edge cryptography at the user side it protects outsourced facts from collusion attack. on the grounds that, do stores its information at csp in encrypted kind and, keys are identified totally to try to do and respected customers group, records confidentiality is ensured. to ensure high-quality-grained get entry to management of outsourced knowledge, the subject has used capability list. public key cryptography and md5 ensure the entity authentication and expertise integrity severally.

public key cryptography and d-h trade protected the facts from Outsiders and wide variety of keys (because in threshold cryptography, there may be one key admire every organization) has reduced in the projected scheme.

S. sanka et.al, has posted a research paper "comfy records get entry to in cloud computing" [3]. on this paper, symmetric key and functionality list scheme attempted to achieve facts confidentiality and access control. on this scheme, facts are encrypted by using symmetric keys which might be acknowledged simplest to facts proprietor and corresponding records users. Csp is locating as garage medium for the encrypted statistics. On account that, the saved facts are encrypted; Csp is not able to see it. Information are in addition encrypted by way of one time secrete consultation-key shared between Csp and user via the diffie-hellman protocol to defend statistics from outsiders during the transmission between csp and user. this scheme no doubt provides the entire records security but there may be related a key corresponding to each person and customers can be massive in number in a few packages. so, quantity of keys increases. these in turn increase the maintenance in addition to security concern of key .so, as to relaxed the records we on occasion make use of such a lot of keys. this greater paintings have an effect on the gadget's performance so, it is recommendable to reduce range of keys.

Sarita kumari has discovered a paper "a research paper on cryptography encryption and compression strategies" [5]. all through this paper records is any fashion of stored digital data. security is concerning the protection of assets statistics protection refers to protective digital privateness measures that rectangular degree applied to prevent unauthorized get entry to computers, personal databases and web sites. cryptography protects customers via supplying practicality for the encryption of facts and authentication of opportunity customers. cryptography will be a fashionable approaches in which of sending very important facts all through a secret method. There are several cryptography strategies offered and amongst them Aes is one in each of the most powerful strategies. The situation of modern-day of information protection gadget includes confidentiality, authenticity, integrity, non repudiation.

In keeping with sultan aldossary et.al, 2016 [6] there are numerous security problems returning with this generation embody troubles associated with the preceding troubles of the internet, network problems, software problems, and storage troubles. Sharing records in cloud when the cloud provider dealer is mistrusted is a hassle, mentioned some method that defends information seen by way of the cloud service provider whereas it's shared amongst several users. This has been carried out to locate the issues that have an effect on confidentiality, integrity, and handiness of records to find an answer for them. those answers can reason safer cloud storage, which is capable of additionally purpose a variety of popularity from the people and additionally the believe at the cloud will growth.

III. MODEL AND ASSUMPTIONS

To recognize proposed scheme higher we take version as an instance of actual existence shape. on this model, there are three important entities: Data owner, cloud service provider and lots of users. records proprietor may be a software program industry who save its facts on to the csp and the customers may be its personnel who view their information from the csp. to begin with, all customers get them self registered at do. We consider that consumer's statistics is despatched securely to do. Do then fills the entries including Uid, Fid and Ar in get admission to right list corresponding to every new consumer. do divides users in corporations on a few similarity foundation like in keeping with their location, department or vicinity and gives encryption keys (Rsa and Sha algorithm), set of rules (lagrange interpolation formulation) and other required things for records outsourcing. this encrypted data are stored at csp. These encryption

algorithms make sure confidentiality and integrity among do and csp. Consumer then request for statistics to Csp. Csp initiates key exchanges with the consumer; if request is truthful algorithms make sure confidentiality between Csp and customers and authenticity of user here user then decrypts the statistics with the aid of the use of threshold cryptography technique.

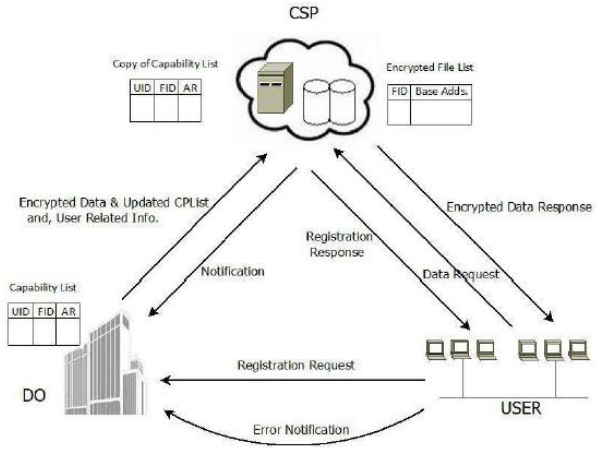

Fig 1: Communication Model in the Proposed Scheme

IV. PROPOSED SCHEME

Problem identification:

There are masses of labor already completed offer to provide protection to information keep at cloud however in almost survey achieved regarding cloud computing the first motive offer for no longer adopting is protection purpose. security remains a first-rate purpose for no longer entirely fundamental cognitive process in cloud. there are also numerous achievable attacks on statistics. they're more or much less proper. information of information owners are processed and maintain at outside servers. So, confidentiality, integrity and get entry to of know-how grow to be extra prone. Since, outside servers are operated by commercial provider providers, records owner cannot agree with on them as they are able to use expertise for their benefits and can ruin businesses of data proprietor. Data owner even can't consider on customers as they may be malicious. facts confidentiality ought to violet via collusion assault of malicious customers and service suppliers.

Design:

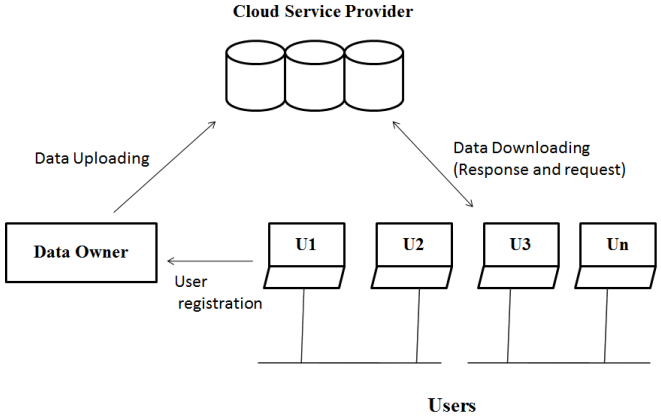

Fig 2: Main Entities for Data Outsourcing

Fig gives a block representation of the general data flow. It has three network entities, viz. the Data Owner, the CSP and users.

1. **Data Owner:** Data owner is responsible for upload the data. It is a network entity that stores data on the cloud server and relies on it for the maintenances and storage of the data.
2. **Cloud Service Provider (CSP):** It is the cloud server that provides significant storage space, resources and maintenance for user data. We have considered CSP as a trusted entity.
3. **User:** User is going to access the data from cloud service provider after the authentications receive from Csp.

Secret sharing scheme (n,n) refers to methods for distributing secret key amongst a group of users, each of whom is allocated a share of the secret key. The secret key can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use on their own. But this scheme take more time for reconstructing secret key when more number of users are present in one group. Threshold cryptography *(t, n)* is the other type of secret sharing scheme there is one data owner and n users. The data owner gives a share of the secret key to the users, but only when specific conditions are fulfilled will the users be able to reconstruct the secret from their shares. The data owner accomplishes this by giving each user a share in such a way that

group of t (for threshold) or more users can together reconstruct the secret key but no group of fewer than *t* users can. Such a system is called a *(t, n)*- threshold scheme (sometimes it is written as an *(n, t)*-threshold scheme). But there are few challenges such as, if threshold value (t) is too small then there is possibility to attack on secret key and if threshold value (t) is too big then it take more time for reconstructing secret key. So, to address these above issues we propose a scheme that uses RSA and SHA algorithm for threshold cryptography in which data owner divides users in group and gives single key to each user groups for decryption of data. Lagrange Interpolation formula is also going to use for distributes the separate key in group for each and every user.

V. Methodology

We assume that our model consists of three entities: a Csp, a Do and masses of customers related to do. initially, all customers are registered at do in the course of registration users send their credentials to do one among the most focus of this model is to authenticate a patron earlier than getting access to carrier. we have a propensity to expect that consumer's credentials are sent securely to do. do then divide customers in agencies and affords encryption keys, tokens, set of rules and one of a kind essential things for cozy communication to user companies in reaction of registration. a consumer gets statistics from csp in a totally personal way once a hit authentication of himself at csp. we tend to assume that csp carries a big functionality and computational strength. we additionally assume that no one will breach the protection of csp. Moreover we will be predisposed to count on that the algorithm this is employed to give you the secrete keys for coding, is secure at do. do have garage functionality to store some documents and facts and, he's going to execute applications conjointly at csp to control his documents and knowledge.

VI. CONCLUSION

An technique which offers safety for statistics outsourced at csp. a few techniques are given to cozy outsourced facts but they may be laid low with having tremendous quantity of keys and collusion attack. viaUsing the brink cryptography on the consumer element, it'll protect outsourced data from collusion attack. when you consider that, do stores its statistics at csp in encrypted kind and, keys are renowned solely to try to do and respected users institution, facts confidentiality are ensured to ensure satisfactory-grained access management of outsourced facts, the theme can use threshold majority.

VII. REFERENCES

[1]. Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma, Sundaram Vats, "Threshold Cryptography Based Data Security in Cloud Computing", IEEE International Conference on Computational Intelligence & Communication Technology, 2015.

[2]. Apurva Gomase, Prof. Vikrant Chole, "Secure system implementation using attribute based encryption", IJATES,Vol.No.03,Special issue No.01,Nov 2015.

[3]. S. Sanka, C. Hota, and M. Rajarajan, "Secure data access in cloud computing," Internet Multimedia Services Architecture and application (IMSAA), 2010 IEEE 4th International Conference on, vol., no., pp.1-6,15-17 Dec. 2010.

[4]. Gauravweni Hedau , Prof. Vikrant Chole , "Implementation of Efficient Approach towards Classification of Semantically Secure Encrypted Data" International Journal of Scholarly Research (IJSR) Vol-1, Issue-2, 2017

[5]. Sarita Kumari, "A research Paper on Cryptography Encryption and Compression Techniques", International Journal Of Engineering And Computer Science, Volume 6 Issue 4 April 2017.

[6]. Sultan Aldossary, William Allen "Data Security, Privacy, Availability and Integrity inCloud

Computing: Issues and Current Solutions", (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 7, No. 4, 2016.

[7]. YatendraSahu, NehaAgrawal, "Scheduling Resources in Cloud using Threshold Values at Host and Data Center level" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (6) , 2015.

[8]. Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing", in Proceedings of the 8th International Conference on Network and Service Management. International Federationfor Information Processing, 2012, pp. 37–45.

[9]. Parikshit N. Mahalle, NeeliRashmi Prasad and Ramjee Prasad, Fellow, IEEE, "Threshold Cryptography-based Group Authentication (TCGA) scheme for the Internet of Things (IoT)", Wireless Communications, Vehicular Technology, Information Theory and Aerospace &Electronics Systems (VITAE), 2014 4th International Conference on11-14 May 2014.

[10]. Carlos Mendes, João Ferreira, Miguel Mira da Silva,"Identifying Services from a Service Provider and Customer Perspectives",International Joint Conference on Knowledge Discovery, Knowledge Engineering, and Knowledge ManagementIC3K 2011.

[11]. Yunchuan Sun, Junsheng Zhang, YongpingXiong, and Guangyu Zhu, "Data Security and Privacy in Cloud Computing", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Volume2014.

[12]. Swapna Lia Anil, Roshni Thanka, " A Survey on Security of Data outsourcing in Cloud", International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013