Data Outsourcing on Cloud using Secret Key Distribution for Privacy Preserving

Pooja Arudkar[1]& Prof. Vikrant Chole[2]
[1&2]Department of Computer Science & Engg.
G.H. Raisoni Academy of Engg & Technology, Nagpur

Abstract:- Cloud computing has turn out to be a trend with the delivery of innumerable advantages. Cloud has come to be a rising widely recognized that brings about diverse era and computing mind for internet at very low rate. Massive garage centres are supplied with the aid of the cloud which may be accessed without problem from any corner of the centre and at any time however there are positive problems and demanding situations faced thru the person at the same time as using cloud computing with reference to protection.

But new stressful situations popped out to ensure Confidentiality, integrity and access control of the records. To deal with the ones troubles we will be inclined to suggest a topic depend that makes use of threshold cryptography internal which records proprietor divides clients in businesses and offers single key to every organization within the imply time, that single key (separate thru approach that will become special mystery key) is distribute to each purchaser of that cluster for decoding of information. The most function of this subject is that cut once more the number of safety key and it additionally make sure that absolutely 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 developing computing paradigm interior which resources of the computing infrastructure are provided as services over the internet. Data safety and get right of entry to control is one in every of the most tough on-going evaluation works in cloud computing because of customers outsourcing their personal data to cloud companies.

Cloud computing is growing as a latest paradigm for this era in the vicinity of engineering and information technology. It's far their attractive offerings like easy to use, online, on demand and pay as use scheme; it is past any doubt useful for tiny and large scale corporations because of it offer services at quite low fee. Cloud might be organisation models which might be the only name for offerings to the person. Purchaser will get entry to those offerings any time at anywhere in the worldwide. Demand of a cloud person can't be foreseen due to the truth it may modification dynamically on runtime.

A cloud makes it possible to get right of entry to information from everywhere inside the global at each time suppliedinternet connection need to be available. It’s far a sort of parallel and allotted device which includes a group of interconnected and virtualized computer systems which might be dynamically provisioned and represented as one or extra unified computing assets primarily based totally on issuer diploma agreements mounted thru negotiation among the provider businesses and customers. There are one-of-a-kind styles of cloud relying on desires. This consists of personal cloud, public cloud, community cloud and hybrid cloud. Public cloud can be accessed using net connection by using manner of any subscriber. Google and Microsoft provide public cloud. A private cloud is constructing for specific enterprise or organisation with gets right of entry to confined to that group. Community cloud is shared among business enterprise with similar cloud requirements. Hybrid cloud is a mixture of as a minimum any of cloud kind.

Cloud support 3 styles of services i.e. package as a service (SaaS), Platform as a Service(PaaS) and Infrastructure as a Service (IaaS). It’ll be deployed in 3 absolutely exquisite approach i.e. non-public cloud, public cloud and hybrid cloud personal cloud is more secure than most of the people cloud.

IaaS clouds, example Amazon, offer virtualized hardware and garage in which the users can deploy their personal applications and services. PaaS clouds, like Microsoft azure, offers a software program development environment for clients who assist them to put into effect and run packages at the cloud. In accordance SaaS cloud there are two forms of cloud, which gives software program applications to the customers. The primary enterprise gives the whole software as a provider to the end customers that are used without any changes or customization. Examples of those varieties of clouds are Google office automation carrier, like Google record or Google calendar. The second one organization presents on-demand for internet offerings to the users, which may be used to construct greater complex packages.

In ultra-modern cryptography, maximum schemes are advanced for a situation with one sender and one receiver. but, there are situations at some point of which numerous receivers (or numerous senders) should be pressured to percent the potential to use a cryptosystem the maximum motivation for threshold cryptography modified into to growth techniques to regulate the multi-sender/multi-receiver scenarios.

Many schemes are given to affirm those protection requirements however they are whole of collusion attack of malicious users and cloud issuer dealer and big computation (because of big no keys). To address those problems a topic is recommended, for the duration of this situation there rectangular degree basically three entities: facts owner (DO), Cloud carrier provider (CSP) and users. Users square measure divided in organizations on a few foundation like location, task, department and corresponding to every organization, there may be one key for encoding and decoding of information. Records could be decrypted as quickly as not less than threshold range of customers can present.

II. Literature Review

Information security is a prime impediment within the manner of cloud computing. Humans are nevertheless fearing to make the most the cloud computing. Some human beings agree with that cloud is risky region and after you send your information to the cloud, you lose entire manipulate over it.

A technique which provides security for information outsourced at CSP. A few tactics are given to cozy outsourced data, but they may be affected by having huge number of keys and collusion attack. By means of making use of the brink cryptography on the user facet, it may defend outsourced facts from collusion attack and also provide authenticity of customers.

Sushil Kr Saroj, et.al, has posted a research paper “Threshold Cryptography primarily based records safety in Cloud Computing” [1]. On this paper, a brand new technique proposed which gives security for statistics outsourced at CSP. A few methods are given to comfortable outsourced statistics but they're suffering from having huge variety of keys and collusion attack. By means of employing the edge cryptography on the user aspect it protects outsourced records from collusion attack. because, DO stores its records at CSP in encrypted form and, keys are recognised simplest to DO and revered customers institution, records confidentiality is ensured. To ensure excellent-grained get right of entry to manipulate of outsourced statistics, the scheme has used functionality listing. Public key cryptography and MD5 make sure the entity authentication and records integrity respectively. Public key cryptography and D-H trade blanketed the records from outsiders and wide variety of keys (because in threshold cryptography, there is a single key similar to each institution) has decreased inside the proposed scheme.

YatendraSahu, NehaAgrawal, has supplied their evaluation paper on “Scheduling assets in Cloud the usage of Threshold Values at Host and information middle level” [2]. At some point of this paper they projected a threshold based broadly speaking compare and stability approach with efficiency allots the cloud computing resources wherever user software dynamically modifications their resource call for with relevancy time. It has shown the relevance of threshold primarily based mostly approach programming strategies to get measurable enhancements in useful resource utilization, server work control and cost-effective approach programming strategies to the cloud server. The deliberate technique may additionally carry fee blessings to cloud companies who are involved with software costs and who are checking out efficiencies with a purpose to be comparatively truly achieved as scenario to migrate the technique because of dynamic call for of computing resource minimized by way of these techniques. This is regularly due to the valuation of transfer between regions, handiness zones and cloud vendors, that all constitute completely extraordinary valuation methods. As useful resource programming algorithmic application internally influences the cloud server load leveling.

S. Sanka et.al, has posted a studies paper “cozy records get admission to In cloud Computing” [3]. in this paper, symmetric key and functionality listing scheme attempted to attain facts confidentiality and get right of entry to manage. On this scheme, facts are encrypted by means of symmetric keys which are regarded most effective to information proprietor and corresponding information users. CSP is locating as garage Medium for the encrypted statistics. On account that, the saved data are encrypted; CSP is unable to see it. Statistics are similarly encrypted via one time secrete session-key shared among CSP and person by using the Diffie-Hellman protocol to protect records from outsiders at some point of the transmission among CSP and consumer. This scheme no question provides the complete facts protection however there's related a key corresponding to each person and customers can be huge in range in some programs. So, number of keys will increase. those in flip growth the maintenance in addition to protection concern of key .So, as to secure the records we once in a while make use of such a lot of keys. This more paintings have an effect on the system’s performance so, it's miles recommendable to lessen quantity of keys.

In 2014, Parikshit N. Mahalle, NeeliRashmi Prasad and Ramjee Prasad, has published a search paper “Threshold Cryptography-based group Authentication (TCGA) scheme for the internet of things (IoT)”, [4]. Internet of factors (IoT) is partner diploma rising paradigm wherever the gadgets around us (persistent and non-chronic) are linked to every different to deliver seamless communication, and discourse offerings. Within the IoT, every tool can't be documented in the quick time due to boundless variety of devices. Equally, it's troublesome to induce receipt in their authentication request at a comparable time. Therefore, relaxed, and cost effective organization authentication subject is needed that authenticates a bunch of devices directly within the context of resource affected IoT. This paper conferred novel Threshold Cryptography-based totally organization Authentication (TCGA) scheme for the IoT that verifies believability of all the devices participating in the cluster communication.

SaritaKumari has found out a paper “A research Paper on Cryptography encryption and Compression techniques” [5]. For the duration of this paper information is any fashion of saved digital facts. Security is concerning the safety of assets. Information protection refers to defensive digital privacy measures that square measure applied to stop unauthorized get entry to to computers, non-public databases and websites. Cryptography protects users by offering practicality for the encryption of facts and authentication of alternative users. Cryptography will be a fashionable ways in which of sending very vital facts for the duration of a secret technique. There are several cryptographically strategies presented and amongst them AES is one in every of the most powerful strategies. The state of affairs of present day of facts safety system consists of confidentiality, authenticity, integrity, nonrepudiation.

in keeping with Sultan Aldossary et.al, 2016 [6] There are several safety issues returning with this technology embody issues related to the preceding troubles of the web, community issues, software problems, and garage problems. Sharing statistics in cloud whilst the cloud provider supplier is mistrusted is a problem, noted some technique that defends records visible by way of the cloud carrier supplier whereas it is shared among several users. This has been performed to find the issues which have an impact on confidentiality, integrity, and handiness of facts to find a solution for them. The ones answers can motive safer cloud garage, which is capable of moreover cause a variety of recognition from the individuals and also the believe on the cloud will growth.

III. Problem Definition

1. There are lots of work already performed offer to produce safety to records keep at cloud however in almost survey done concerning cloud computing the primary cause offer for no longer adopting is security cause.
2. Security is still a chief reason for now not thoroughly fundamental cognitive technique in cloud. There are also numerous doable assaults on data. They are greater or less proper.
3. Information of information proprietors are processed and maintain at external servers. So, confidentiality, integrity and access of know-how emerge as additional vulnerable.
4. When you consider that, external servers are operated by way of business provider providers, records proprietor can’t agree with on them as they could use know-how for his or her benefits and might damage agencies of information owner.
5. Information owner even can't agree with on customers as they may be malicious. Information confidentiality may want to violet via collusion attack of malicious customers and service providers.

IV. Objective

1. There is a motive for exploitation threshold cryptography is to supply extra safety to the information used by secret proportion scheme. At some point of this scheme users are divided into group consistent with their region, branch and their project.
2. There is a single key for encoding and decoding of statistics. Each person in the institution stocks components of the important thing. Information may be encrypted as soon as not less than threshold range of users can gift.
3. This scheme not solely provides facts confidentiality by all means that but also reduces the range of keys. This is often a safe and comfort methodology to provide safety to records.

V. Proposed Scheme

To understand proposed scheme better we take an example of real life scenario, DO may be a software industry who stores its data on to the CSP and the users may be its employees who view their data from the CSP. DO divides users in groups on some basis such as project basis and encrypts the data of each group with a single public key and, it gives parts of the secret key (KT) to each user of the group. DO compute digest of data by using SHA hash algorithm and then encapsulates the digest and data using the secret key (KT). This in turn, provides strong data confidentiality and integrity. DO then fill the entries such as UID, FID and AR in Capability List corresponding to each new user. DO then encrypts Capability List and encapsulated things with its private key after that public key of CSP and, then sends all things to CSP. These encryptions ensure confidentiality and authentication between DO and CSP.

Algorithm 1: Procedure to be followed by CSP after getting encrypted File and Capability List from DO.

Step 1: CSP stores Encrypted Data and Capability List which are received from DO.
Step 2: CSP updates the Encrypted File List.
Step 3: CSP updates Capability List.

Algorithm 1 describes the process what CSP do after getting encrypted data and Capability List from the DO. CSP decrypts the message using its own private key and the public key of data owner and stores the encrypted data and Capability List in its storage. CSP then updates the encrypted File List and Capability List. Since, data are encrypted using private key (Pr) which is known only to DO and respected user group, CSP can't see data even though user's credential comes through it.

Algorithm 2: Procedure to be followed after a new File creation

Step 1: DO updates Capability List means add UID, FID, AR.
Step 2: Now, DO encrypts the CPList, Encrypted File, private key and sends these to the CSP
Step 3: CSP Updates its copy of the Capability List, Encrypted File List and sends public key(Pu) to indented user group
Step 4: Now, the user can send actual access request for that File directly to CSP

Algorithm 2 illustrates the procedure required after a new File creation. When a new File is created, DO fills entries for that File in Capability List containing UID, FID and AR. DO generates a private key (Pr) and encrypts File and with the public key (Pu) decrypts file by user. Now, DO encrypts the updated CPList, Encrypted File and private key (Pr) with its private key after that public key of CSP and sends these to the CSP. When CSP receives these, it updates Capability List, Encrypted File List and sends encrypted public key (Pu) to respective user group. Users of the user group then decrypt the message and get their own parts of the secret key (KT).

Algorithm 3: Algorithm for secure data exchange between CSP and User by using Lagrange Interpolation formula.

Step 1: User sends data access request to CSP

Send(UID, FID, AR))

Step 2: CSP matches UID, FID, AR with CP List stored at it.

If(match)

Go to step (3)

else

Go to step (6)

Step 3: CSP initiates for key with that User and shares secret key(KS)

Step 4: CSP generate secret key and sends it to User Send(((Fi)))

Step 5: User decrypts the File and calculates the message digest of that File

If

Calculated digest matches with stored digest then File is original

else

File is modified and User sends Error Notification to DO

Step 6: CSP sends 'invalid request' message to User

Algorithm 3 describes how data are exchanged securely between CSP and the user by use of Lagrange Interpolation formula. We assume that the secret key (KT) is shared between CSP and the user by Lagrange Interpolation formula. Now, CSP encrypts the encrypted File (Fi) and its digest (Di) with the secret key (KT) and sends it to the user. This over encryption ensures the confidentiality of the message between cloud service provider and the user.

Algorithm 4: Algorithm for Decryption of a File for User 1

Step 1: User 1 receives Encrypted File

Step 2: User 1 will also update the part of key and other user who is part of that threshold group give their side of part of key.

Step 3: After receiving partial key set successful authentication is done.

Step 4: After getting keyset then that user who is going to access that file will going to download the file.

The user then decrypts the message (user decrypts the message according to algorithm 4) and calculates the digest of File and then matches it with stored digest. If digest matches, File is original otherwise File is modified by outsiders and user then sends an error notification message to DO.

In proposed system the RSA and SHA algorithm is used to create one time encryption key between CSP and user. DO then divides users in groups and provides single keys, algorithm (Lagrange Interpolation formula) is applied in groups key and other necessary things for secure communication to user groups in response of registration.

Symbol	Description
DO	Data Owner
CSP	Cloud Service Provider
Pu	Public Key
Pr	Private Key
KT	Secret Key
Ek	Encryption
Dk	Decryption
PuCSP	Public Key of CSP
PrCSP	Private Key of CSP
PuDO	Public Key of DO
PrDO	Private Key of DO
PuUSR	Public Key of User
PrUSR	Private Key of User
Fi	ith File
Di	ith File Message Digest
d	Number of Shares
UID	User Identity
FID	File Identity
AR	Access Right
CPList	Capability List
M	Message
PKS	Partial Key Set
KTi	ith User's partial key
OR	OR operation of Gate
SHA	Hash Algorithm
XA/B	Chosen Secret Key
YA/B	Calculated Public Key

VI. Conclusion:

A technique which offers safety for statistics outsourced at CSP. A few techniques are given to cosy outsourced facts but they may be laid low with having tremendous quantity of keys and collusion attack. Using the 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.

The proposed scheme is useful for those applications where works are done in team and group such as in software industries. You may think proposed scheme has limited applications but it is not as such. It is applicable all where you can group users on some basis and can apply threshold cryptography technique. Such as software and hardware industries, institutes, banks and medicals fields. There is provision of hierarchy of access in this scheme which makes this scheme more useful and realistic. For Example, an university has vice-chancellor, hods, teachers, clerklier-staff and students. Each one has different level of access right.

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] 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.

[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] 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.

[5] SaritaKumari, “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] 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.

[8] 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.

[9] 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.

[10] ApurvaGomase, Prof. Vikrant Chole, ”Secure system implementation using attribute based encryption”, IJATES,Vol.No.03,Special issue No.01,Nov 2015.

[11] GauravweniHedau ,Prof.VikrantChole , “Implementation of Efficient Approach towards Classification of Semantically Secure Encrypted Data” International Journal of Scholarly Research (IJSR) Vol-1, Issue-2, 2017.

[12] SwapnaLia Anil, RoshniThanka, “A Survey on Security of Data outsourcing in Cloud”, International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.