ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

CLOUD BASED SECURE STORAGE MANAGEMENT FOR DYNAMIC GROUPS

[1]Dr.N.PARTHEEBAN [2]Dr.AHMED MUDASSAR ALI [3]Dr.N.SANKAR RAM[4]Dr.D.HEMANAND

[1]Associate Professor, Department of CSE, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology,Chennai -62.

[2]Associate Professor, Department of IT, S.A.Engineering College, Thiruverkadu, Chennai -77.

[3]Professor, Department of CSE, Sriram Engineering College, Veppampattu, Tiruvallur, Chennai-602024

[4] Assistant Professor, Department of CSE, Sriram Engineering College, Veppampattu, Tiruvallur, Chennai-602024

E-mail: [1]knparthi78@gmail.com ,[2]ahmedmudassarali@saec.ac.in[3]n_sankarram@yahoo.com,

[4]d.hemanand@gmail.com

Abstract: *Cloud computing provides an economical and efficient solution for sharing group resource among the cloud users. Encrypted data search allows cloud to offer fundamental information retrieval service to its users in a privacy preserving way. In most existing schemes, search result is returned by a semi-trusted server and usually considered authentic. Unfortunately, sharing the data in the multi-owner group while preserving data and identify privacy from an untrusted cloud is still a challenging issues. By leveraging group signature and dynamic broadcast encryption technique any cloud user can anonymously share data with others.cloud typically hosts large outsourced data of users in its storage. The verification cost should be efficient enough for practical use, i.e., it only depends on the corresponding search operation, regardless of the file collection size For example, Alice can upload authenticated data to "the cloud" which then performs some specified computational over this data and send the output to the Bob with the tag that convince Bob. Alice and Bob only share a random secret key. The result is the algorithm that we know of to compute correlations over thousands of data streams in real time.*

Key Words:Index terms: Cloud computing, multi owner, secret random key, data sharing,Privacy- preserving

INTRODUCTION: The past few years have witnessed the proliferation of streaming data generated by a variety of applications/systems, such as GPS, Internet traffic, asset tracking, wireless sensors, etc. Retaining a local copy of such exponentially-growing volume of data is becoming prohibitive for resource-constrained companies/ organizations, let alone offering efficient and reliable query services on it. Consider a stream-oriented service (e.g., market analysis, weather forecasting and traffic management), where *multiple* resource-constrained sources continuously collect or generate data streams, and outsource them to a powerful external server, e.g. cloud, for desired critical computations and storage savings. For example, using inner product computation over any two outsourced stock

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

data streams from different sources for correlation analysis, a stock market trader is able to spot the arbitrage opportunities.

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. Cloud computing is recognized as an alternative to traditional information technology due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures.

One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans.

To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable.

Our contributions. To solve the challenges presented above, we propose Mona, a secure multi-owner data sharing scheme for

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

dynamic groups in the cloud. The main contributions of this paper include:

1. We propose a secure multi-owner data sharing scheme. It implies that any user in the group can
securely share data with others by the untrusted cloud.
2. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily achieved through a novel revocation list without updating the secret
keys of the remaining users. The size and computation overhead of encryption are constant and
independent with the number of revoked users.
3. We provide secure and privacy-preserving access control to users, which guarantees any member in a
group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.
4. We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

RELATED WORK:

Secure search technique has been achieved in both symmetric and asymmetric settings with a variety of search functionalities investigated in Static Search. In the symmetric setting, proposed an efficient secure single-keyword search scheme, and gave a formal security notion, i.e., security against chosen- keyword attack and a stronger notion of adaptive security against chosen-keyword attack . To enrich the search functionality, secure multi-keyword search was realized improved the search efficiency and accuracy using a tree based index structure and the cosine similarity measure in the vector space model. In the public key scenario, presented the first public key encryption with keyword search scheme constructed from identity-based encryption. Recently, proposed the attribute-based keyword search scheme to realize fine-grained owner-enforced search authorization. Note that the above schemes only support static data, and are secure against a semi-trusted server. Dynamic Search proposed a dynamic secure search scheme but the bloom filter based index may introduce false positive into the final search result also presented a dynamic search solution with linear search time. Data insertion and deletion on the outsourced dataset. Later they accelerated the search process by using secret key technique . However, these works will not be secure against a malicious adversary, and users cannot verify the authenticity of returned search result a dynamic encrypted data search scheme with small search privacy leakage, which enables result verification for single keyword search. It is worth noting that most of these search verification mechanisms are heuristic constructions without evaluating the practical performance, especially for large-scale dataset stored in the cloud. In addition, no scheme can achieve conjunctive, dynamic, and publicly/privately verifiable search. [5] discussed that the activity related status data will be communicated consistently and shared among drivers through VANETs keeping in mind the end goal to enhance driving security and solace. Along these

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

lines, Vehicular specially appointed systems (VANETs) require safeguarding and secure information correspondences. Without the security and protection ensures, the aggressors could track their intrigued vehicles by gathering and breaking down their movement messages. A mysterious message confirmation is a basic prerequisite of VANETs. To conquer this issue, a protection safeguarding confirmation convention with expert traceability utilizing elliptic bend based chameleon hashing is proposed. Contrasted and existing plans Privacy saving confirmation utilizing Hash Message verification code, this approach has the accompanying better elements: common and unknown validation for vehicle-to-vehicle and vehicle-to-roadside interchanges, vehicle unlinkability, specialist following capacity and high computational effectiveness

Multi-key Setting. Recently, a multi-key non interactive verifiable computation scheme was proposed in followed by a stronger security guarantee scheme [23]. In their constructions, ncomputationally-weak users outsource to an untrusted server the computation of a function f over a series of joint inputs (x(i)1 , x(i)2 , ..., x(i)n) without interacting with each other, where i denotes the computation. In their schemes, after the generation of system parameters, data sources Pj(j , [1, n]) outputs an encoded function f to the server. Then for the computation, Pj outsources the encoding of x(i)j to the server and computes a secret (i)j for the verification. However, these schemes may not be applied to the stream setting since sources lost data control after the outsourcing and thus cannot generate the corresponding secrets for the verification. Besides, both of them based on FHE are not practically efficient. As shown in it takes at least 30 seconds to run one bootstrapping operation of FHE for weaker security parameter on a high performance machine.

ALGORITHM:

- KeyGen(1) (pkj , skj): A probabilistic algorithm run by each machine Mj takes a security Parameter as input, and outputs a public key pkj and a secret key skj .
- TagGen (skj , i,Xj,i)j,i: A (possibly) probabilistic algorithm run by machine Mj, takes as input its secret key skj , the current discrete time i and data Xj,i, and outputs a publicly verifiable tag j,i. Evaluate(FIP,Xi,Xj) ¨ res: Let Xi ={Xi,1,Xi,2, ...,Xi,n} and Xj = {Xj,1,Xj,2, ...,Xj,n} denote the outsourced data streams of machines Mi and Mj, respectively. This deterministic algorithm is run by the server to compute the inner product of streams Xi and Xj . It takes as inputs the inner product function FIP, two data streams Xi and Xj , and outputs a computation result res.

• GenProof (FIP, i, j ,Xi,Xj) → : Let i and j denote the tag vectors for Xi and Xj generated by machine Mi and machine Mj, respectively. This algorithm is run by the server to generate a proof for the result res. It takes as input the inner product function FIP, two tag vectors I and j , as well as two data streams Xi and Xj , and outputs a proof .

• CheckProof (FIP, pki, pkj , res,) → 0, 1: A deterministic algorithm is run by

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

the client to check the correctness of res. It takes as input the function FIP, two public keys pki and pkj , the result res, as well as the proof , and outputs 1 (accept) or 0 (reject).

$\mathrm{KeyGen}(1^\kappa)$:
1. for $j = 1$ to l do
2. choose a random number $sk_j = s_j \in Z_q^*$ as the secret key
3. compute $pk_j = g^{s_j}$
4. output (pk_j, sk_j)
5. end for

$\mathrm{TagGen}(sk_j, i, \mathcal{X}_{j,i})$:
1. compute $\sigma_{j,i} = (g_1^{h_1(M_j,i)} g_2^{h_2(M_j,i)} g_3^{\mathcal{X}_{j,i}})^{sk_j}$
2. output $\sigma_{j,i}$

$\mathrm{Evaluate}(\mathcal{F}_{\mathcal{GS}}, \mathcal{X}_j)$:
1. compute $res = \sum_{i \in \Delta} \mathcal{X}_{j,i}$
2. output res

$\mathrm{GenProof}(\mathcal{F}_{\mathcal{GS}}, \sigma_j, \mathcal{X}_j)$:
1. compute $\pi = \prod_{i \in \Delta} \sigma_{j,i}$
2. output π

$\mathrm{CheckProof}(\mathcal{F}_{\mathcal{GS}}, pk_j, res, \pi)$:
1. set $S_\Delta = (S_1, S_2)$
2. compute $S_1 = \sum_{i \in \Delta} h_1(M_j, i)$ and $S_2 = \sum_{i \in \Delta} h_2(M_j, i)$
3. if $(e(\pi, g) = e(g_1^{S_1} g_2^{S_2} g_3^{res}, pk_j))$ then
4. output 1
5. else
6. output 0
7. end if

LITERATURE SURVEY:

I. Cloud Computing Interoperability Approaches – Possibilities and Challenges

The Cloud Computing Interoperability (CCI) is a hot re-search topic and has been addressed by many scientists, architects, groups etc. A lot of different approaches and possible solutions are published, but there is no accepted standard or model yet. This paper is a survey of the most influential published CCI models and discusses their pos-sibilities and challenges. The accent in this paper is set to analysis of the Software as a Service (SaaS) CCI model based on adapters. The current state of the cloud computing market and the results of recent Cloud Computing (CC) market surveys are also included in our analysis. The presented conclusion addresses the increasing trend in the usage of cloud computing and the lack of visible result to achieve cloud computing interoperability. So the next logical

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

step is to create adapters to achieve interoperability at the SaaS level.

II. Cloud Computing and Software Agents: Towards Cloud Intelligent Services

Cloud computing systems provide large-scale infrastructures for high-performance computing that are "elastic" since they are able to adapt to user and application needs. Clouds are used through a service-oriented interface that implements the *-as-a-service paradigm to offer Cloud services on demand. This paper discusses Cloud computing models and architectures, their use in parallel and distributed applications, and examines analogies, differences and potential synergies between Cloud computing and multi-agent systems. This analysis is lead having in mind the goal of implementing high performance complex systems and intelligent applications by using of Cloud systems and software agents. The convergence of interests between multi-agent systems that need reliable distributed infrastructures and Cloud computing systems that need intelligent software with dynamic, flexible, and autonomous behavior can result in new systems and applications.

III. Agent Based Framework for Scalability in Cloud Computing

Cloud computing focuses on delivery of reliable, secure, fault tolerant, sustainable, and scalable infrastructures for hosting internet-based application services. These applications have different composition, configuration, and deployment requirements. Cloud service providers are willing to provide large scaled computing infrastructure at a cheap prices. Quantifying the performance of scheduling and allocation policy on a Cloud infrastructure (hardware, software, services) for different application and service models under varying load, energy performance (power consumption, heat dissipation), and system size is an extremely challenging problem to tackle. This problem can be tackle with the help of mobile agents. Mobile agent being a process that can transport its state from one environment to another, with its data intact, and is capable of performing appropriately in the new environment. This work proposes an agent based framework for providing scalability in cloud computing environments supported with algorithms for searching another cloud when the approachable cloud becomes overloaded and for searching closest datacenters with least response time of virtual machine (VM).

IV. Resource Allocation and Scheduling in the Cloud

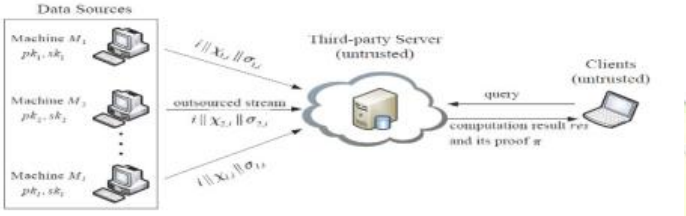
Recently, there has been a dramatic increase in the popularity of cloud computing systems that rent computing resources on-demand, bill on a pay-as-you-go basis, and multiplex many users on the same physical infrastructure. These cloud computing environments provide an illusion of infinite computing resources to cloud users so that they can increase or decrease their resource consumption rate according to the demands. At the same time, the cloud environment poses a number of challenges. Two players in cloud computing environments, cloud providers and cloud users, pursue different goals; providers want to maximize revenue by achieving high resource utilization, while users want to

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

minimize expenses while meeting their performance requirements. However, it is difficult to allocate resources in a mutually optimal way due to the lack of information sharing between them. Moreover, ever-increasing heterogeneity and variability of SYSTEM ARCHITECTURE:

the environment poses even harder challenges for both parties. This paper reviews certain papers on resource management and job scheduling in cloud computing



3 EXISTING SYSTEM:

File Stream upload with Single Key Verification is risky factor. File Data may easily hack or theft by the untrusted Server. The outsourced computation is data cannot be achieved in Single key Algorithm. A probabilistic calculation keep running by every machine takes a tag alone as information, and yields an open key and a mystery key

DRAWBACKS IN EXISTING SYSTEM:

- Can Upload Single Data at a time.
- Produce Single key for Security of each parameters

4 PROPOSED SYSTEM:

The outsourced computation is data is more secured. Public verification property is banned. The publicly and efficiently verify the inner product evaluation over the outsourced data streams under multiple keys still make more security and accessing data is efficient. A probabilistic calculation keep running by every machine takes a security parameter _ as information, and yields an open key and a mystery key. A (perhaps) probabilistic calculation keep running by machine, takes as info its mystery key, the current discrete time and information and yields a freely unquestionable tag.

ADVANTAGES IN PROPOSED SYSTEM:

- Multi-key scenario allows multiple data sources with different secret keys
- To upload their endless data.
- Corresponding computations to a third party

5 FUTURE CONCEPT : -

- Furthermore, any keyless customer can freely check the legitimacy of the returned calculation result.
- Security examination shows that our arrangement is provable secure under the CDH supposition in the unpredictable prophet model.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

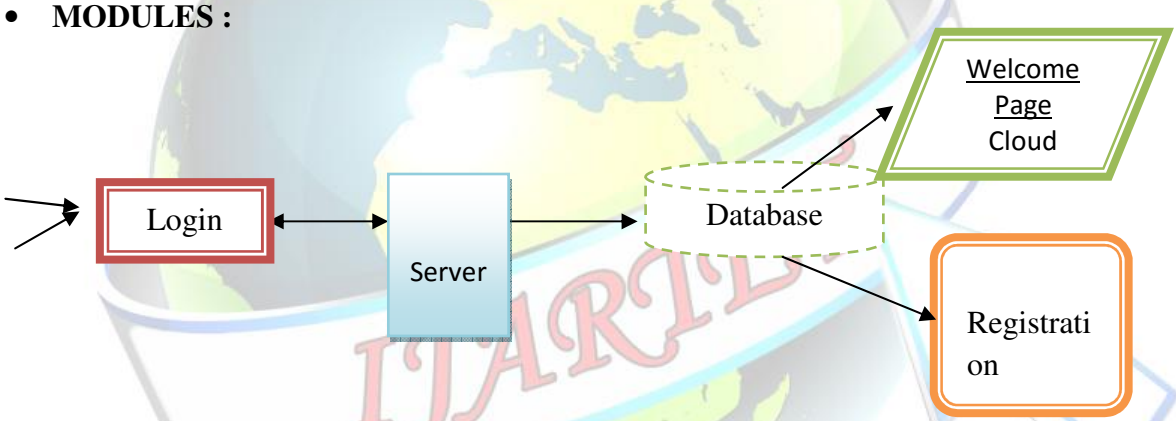
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

Results show that our tradition is in every practical sense gainful to the extent both communication and computation cost.

- Sum Algorithm

- Sum Algorithm present a publicly verifiable group by which servers as a building block for verifying the inner product of dynamic vectors under two different keys.
- Inner Data Access with two different keys make the data more secured
- **SYSTEM IMPLEMENTATION**
- **MODULES :**

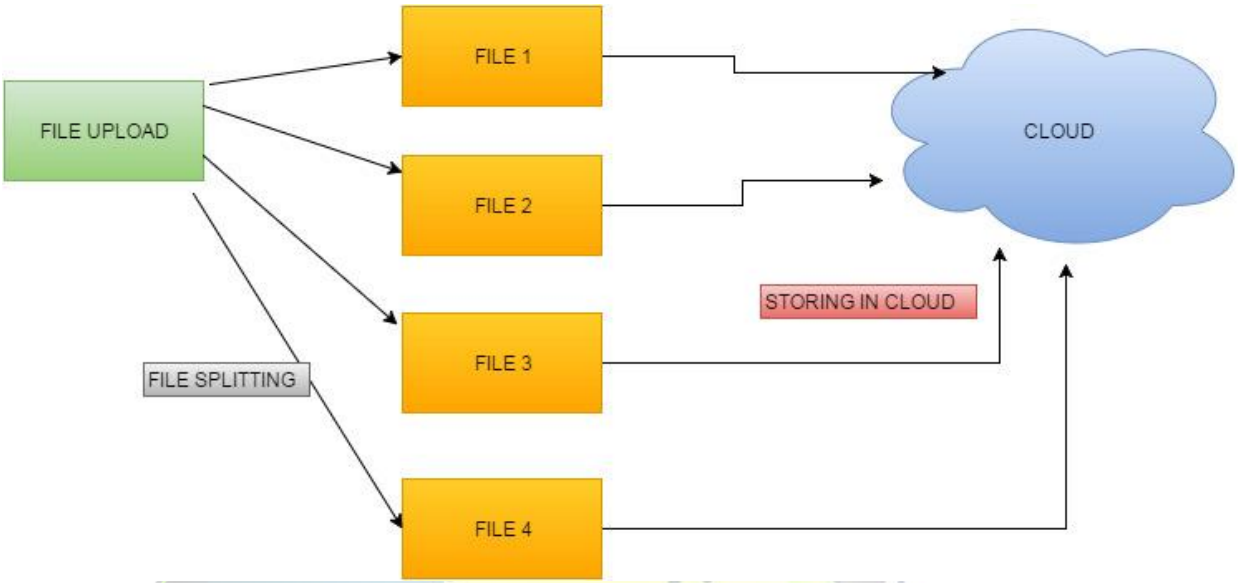
1. User interface : To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. . Logging in is usually used to enter a specific page.



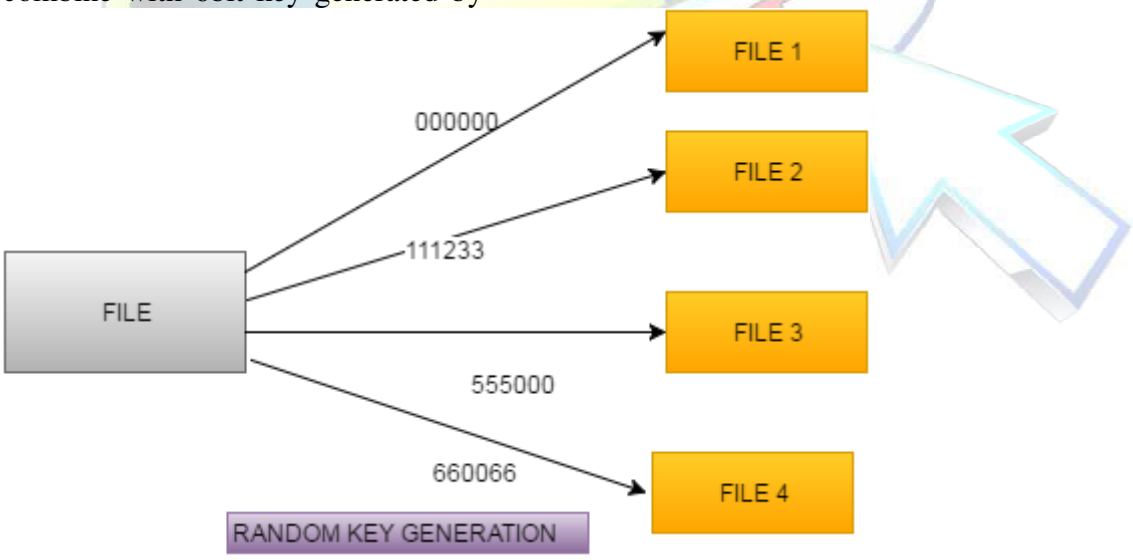
2. File Splitting: In this module the file being uploaded will be converted from a plain text to cipher text i.e., encrypting the normal file to cipher text file and it will be split into 4 parts with 4 tokens.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018



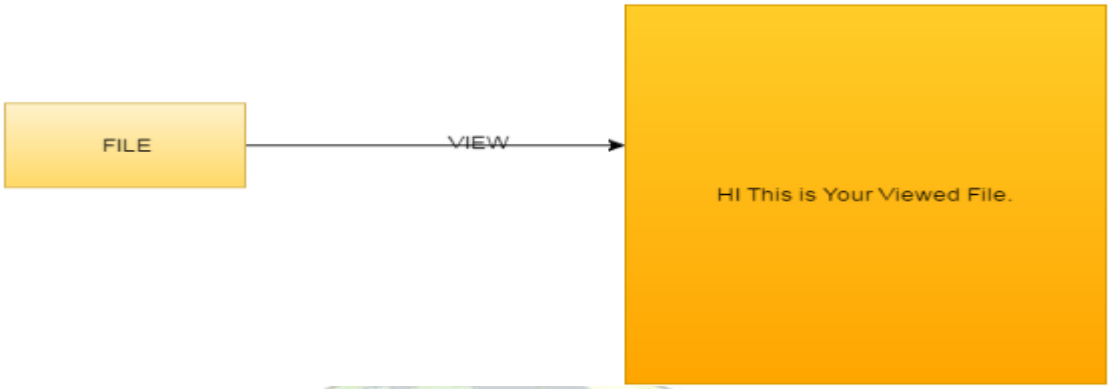
3. Multiple Token Generation: In this module the file being split into 4 parts contains 2 bit token for each split file which will be then combine with 6bit key generated by the random Manner for file encryption we used DES(DATA ENCRYPTION STANDARD)



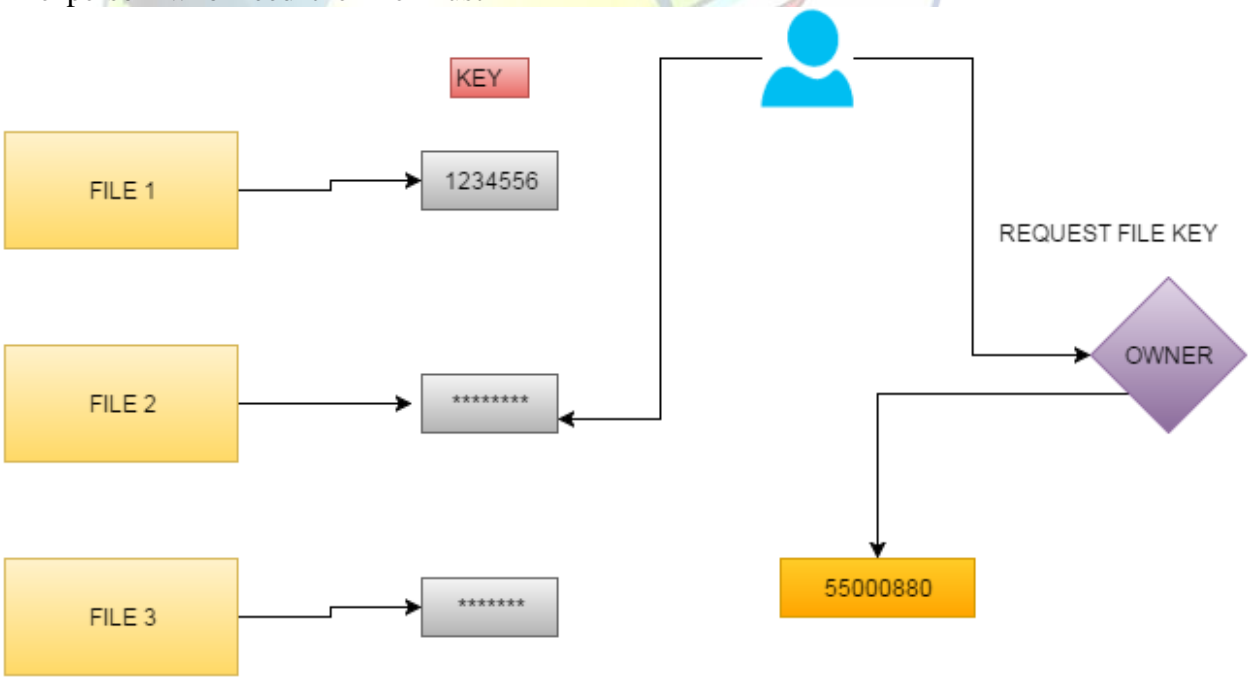
4. View/Read File: For reading each file which have been uploaded and split into 4 parts we should be owner of the file otherwise we should know the four 8bit tokens which have been combined by random algorithm after reading the file you can also download the file otherwise with wrong tokens you can get only cipher text of the content.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018



5. REQUESTING/RESPONSE FILE:Requesting a file means as you are not owner of the file but you need to read or download the file that is possible only by owner approval. The person who need the file must be requested to file owner for the tokens once the tokens have been given by the owner the person can able to read/view the file with the token otherwise the person can't able to get the file.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 1, January 2018

Conclusion & Future Enhancement

A secure data sharing scheme for dynamic groups in an untrusted cloud have been designed. The user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well. Compared with the existing works under the single-key setting, our scheme aims at the more challenging multi-key scenario, i.e., it allows multiple data sources with different secret keys to upload their endless data streams and delegate the corresponding computations to a third party server, while the traceability can still be provided on demand.

References:

[1] The NIST Definition of Cloud Computing. National Institute ofStandards andTechnology,Commerce.http://www.csrc. nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

[2] M. Armbrust et al. Above the clouds: A Berkeley view of cloudcomputing. Tech. Rep. UCB/EECS-2009-28, EECS Department,
U.C. Berkeley, Feb 2009.[3] D. Bernstein et al. Blueprint for the Intercloud- Protocols andFormats for Cloud Computing Interoperability. Proc. 4th Int.Conf. Internet and Web Applications and Services pp. 328–336.,Venice, May 2009.[4] M. Wooldridge, An Introduction to Multiagent Systems, JohnWiley& Sons, 2002.

[5] Christo Ananth, Dr.S. Selvakani, K. Vasumathi, "An Efficient Privacy Preservation in Vehicular Communications Using EC-Based Chameleon Hashing", Journal of Advanced Research in Dynamical and Control Systems, 15-Special Issue, December 2017,pp: 787-792.

[6] K. M. Sim, Complex and concurrent negotiations for multipleinterrelated e-markets, IEEE Trans. Cybernet. 43 (1), pp. 230–245 2013.

[7] S. Son and K. M. Sim, A price-timeslot negotiation for cloudservice reservation, IEEE Trans. Syst. Man Cybernet.B 42 (3), pp.713–728, 2012.

[8] J. O. Gutierrez-Garcia and K. M. Sim, Agent-based cloud servicecomposition, Appl. Intell. 38 (3), pp. 436–464, 2013.

[9] J. O. Gutierrez-Garcia and K. M. Sim, Family of heuristics foragent-based elastic cloud bag-of-tasks concurrent scheduling,
Future Generat.Comput.Syst. 29 (7), pp. 1682–1699, 2013.

[10] J. O. Gutierrez-Garcia and K. M. Sim, Agent-based cloudworkflow execution, Integr. Comput. Aided Eng. 19 (1), pp. 39–56, 2012.