SECURE DATA SHARING IN CLOUD BASED ENVIRONMENT USING RSA, AES AND TIME SECEDULING

L.Hemalatha[1] , D.B.Shanmugam[2], A.Vignesh[3]
[1]MPhil., Research Scolar, Dept.Sci,Dr.MGR.Chockalingam Arts College,Arni.
[2]Asst.Prof., Dept of Comp.Sci, Dr.MGR.Chockalingam Arts College,Arni.
[3]Asst.Prof. , SRM Institute of Science and Technology.,Ramapuram campus

Received: May 24, 2018 Accepted: July 08, 2018

ABSTRACT *Data outsourcing and data backup are carried out in cloud by the data owner and maintained by third-party cloud storage service providers so as to reduce the cost for data management. To protect the data from the unauthorized user, data is stored in an encrypted form security is a major concern for the outsourced or backup data. This thesis introduces multiple KDM to handle the data with different access policies to avoid insider attack. The algorithms like RAS, AES and TIME SECEDULING. The data owner have to register with all personal details they have to fill with in a allocated time that data owner have to select one particular group because here we have some categorized groups for storing a file in cloud .The data owner have to select one particular group after selecting that all details will be stored in cloud after storing the details will be sent to service provider then if service provider accept means then only that particular user can get the access right. If any user what to get any file from the cloud they can able to get with in the allocated time by the service provider.*

Keywords: *Secure, RSA, AES, TIME SCHEDULING, Encryption , Decryption*

I.INTRODUCTION

One of the fundamental trends of cloud computing is to use the cloud services in a pay-as-you-bypass manner [1]. Also cloud offers an infinite garage area for consumer to keep their data. Therefore cloud garage offers the manner for a ways off facts backup, simply so person can capable of retrieve the statistics at any time the usage of the cloud services.. There are more case research which can be related to cloud garage for faraway statistics backup [2]. Additionally people can keep their private statistics to the cloud using Dropbox and Google force and so forth [3, 4]. In recent times greater variety of peoples are the usage of gear like Dropbox to store their statistics in cloud. However, the proposed work keep in mind the security concerns in storing the touchy facts in cloud that's maintained by using 0.33 birthday party cloud offerings. In proposed work, two security problems are taken into consideration specially. First, make certain that most effective legal events have get admission to the outsourced information in cloud via green key distribution mechanism and get admission to coverage. second, to assure cozy statistics get entry to put into effect cryptography schemes for presenting protection while user Upload/download data from cloud offerings. By mentioning these method RSA and AES algorithm for accomplishing the proposed troubles. Additionally carry out several cryptography key operations to protect the facts that is accessed from the cloud. The proposed protocol is relevant for popular garage backups where upload/download of facts takes place with the help of backend interface. Numerous research [5] are related to the safety of outsourced data the usage of cryptographic techniques. Wang et al. [6] proposed an auditing machine that allows the user to verify the integrity of outsourced information. Wang et al. [7] got here up with. A cozy outsourced records access mechanism with get entry to rights. Yunetal. [8] referred to about the integrity and privateness on an outsourced records the usage of hash-based totally mechanism.. RSA is the most famous public key set of guidelines. Rivest, Shamir and Adleman [9] invented this set of policies in which each public and private key's used for encryption and decryption. All of the messages are encrypted the usage of the general public key and it's miles despatched to the receiver. The receiver uses the non-public key to decrypt the message. Yellammaet. Al[11] proposed a way to at ease facts in cloud the usage of RSA. Joan Daemen and Vincent Rijment [10] invented AES a symmetric set of rules. AES makes use of the identical key for each encryption and decryption of messages. The last paper is prepared as follows: in section 2, talk the proposed works. In phase 3, describe the implementation details and look at the overall performance of our proposed artwork. Eventually, segment 4 gives the belief of our paintings. Cloud: Statistics outsourcing and statistics backup are accomplished in cloud by way of the information proprietor. To defend the

information from the unauthorized person, data is saved in a form of encryption in cloud. Confidentiality is accomplished by way of the usage of storing the statistics in an encrypted shape. The cryptographic operation and also the upload and down load report operation are completed the usage of our proposed approach. So there is no a good deal involvement of cloud precise operation in our work. KDM: The important problem Distribution supervisor (KDM) is acted as depended on 0.33 party in which all the cryptographic related operations are completed right right here. ACL is also maintained in KDM for storing policy for person documents. Whenever customer desires to upload or down load the file in cloud, first if any user is going to sign up with KDM then KDM: verifies for authentication. KDM can be maintained with the useful aid of manner of the enterprise company itself to generate take shipping of as proper with for the user who are gaining access to the statistics.

III. LITERATURE SURVEY

Security Issues for Cloud Computing: Security issues for the cloud computing is the vast accept to come through, but there are many issue like Integrity, Confidentiality, Availability, Map reduce. Here the discussion is related to the trending issues and how to build the trusted applicaion from untrusted component of secure cloud computing .

A High-Availability and Integrity Layer for Cloud Storage: HAIL a distributed cryptographic system that allows a set of servers to prove to a client that a stored file is intact and retrievable. HAIL is efficiently computable by servers and highly compact typically tens or hundreds of bytes, irrespective of file size. HAIL improves on the security and efficiency of existing tools, like Proofs of Retrievability (PORs) deployed on individual servers. We propose a strong, formal adversarial model for HAIL, and rigorous analysis and parameter choices. We show how HAIL improves on the security and efficiency of existing tools, like Proofs of Retrievability (PORs) deployed on individual servers.

Deadline constraint heuristic-based genetic algorithm for workflow scheduling in cloud: Task scheduling and resource allocation are the key challenges of cloud computing. Compared with grid environment, data transfer is a big overhead for cloud workflows. So, the cost arising from data transfers between resources as well as execution costs must also be taken into account during scheduling based upon user's Quality of Service (QoS) constraints. In this paper, we present Deadline Constrained Heuristic based Genetic Algorithms (HGA) to schedule applications to cloud resources that minimize the execution cost while meeting the deadline for delivering the result. Each workflow's task is assigned priority using bottom-level (b-level) and top-level (t-level).To increase the population diversity, these priorities are then used to create the initial population of HGAs. The proposed algorithms are simulated and evaluated with synthetic workflows based on realistic workflows. The simulation results show that our proposed algorithms have a promising performance as compared to Standard Genetic Algorithm (SGA).

Providing Security and Integrity for Data Stored In Cloud Storage: A scheme by which there provided a secure saving of confidential data in cloud storage in an efficient manner which requires low computational power and time and disallowing hacker from penetrating into private data storage. So there provided a simple and easy integrity checking mechanism when compared to other already present one by which verification can be done whether data is not corrupted and deleted or modified ours is an efficient. Integrity checking mechanism is simple that it does not take more computational power. This mechanism even prevents the TPA who maintains our data in cloud storage from editing our file.

Deadline-constrained workflow scheduling algorithms for Infrastructure as a Service Clouds : The advent of Cloud computing as a new model of service provisioning in distributed systems encourages researchers to investigate its benefits and drawbacks on executing scientific applications such as workflows. One of the most challenging problems in Clouds is workflow scheduling, i.e., the problem of satisfying the QoS requirements of the user as well as minimizing the cost of workflow execution. We have previously designed and analyzed a two-phase scheduling algorithm for utility Grids, called Partial Critical Paths (PCP), which aims to minimize the cost of workflow execution while meeting a user defined deadline. However, we believe Clouds are different from utility Grids in three ways: on-demand resource provisioning, homogeneous networks, and the pay-as-you-go pricing model. In this paper, we adapt the PCP algorithm for the Cloud environment and propose two workflow scheduling algorithms: a one-phase algorithm which is called IaaS Cloud Partial Critical Paths (IC-PCP), and a two-phase algorithm which is called IaaS Cloud Partial

Critical Paths with Deadline Distribution (IC-PCPD2). Both algorithms have a polynomial time complexity which make them suitable options for scheduling large workflows. The simulation results show that both algorithms have a promising performance, with IC-PCP performing better than IC-PCPD2 in most cases.

III. PROPOSED ARCHITECTURE

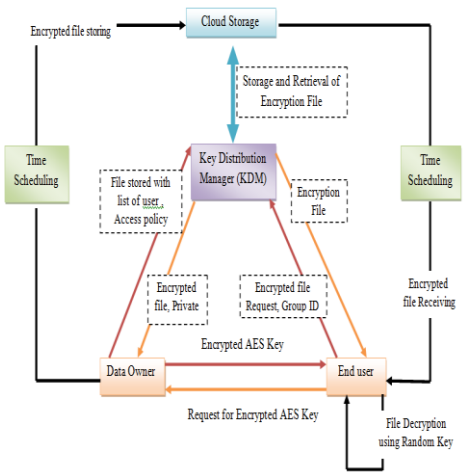

Fig 3: PROPOSED ARCHITECTURE

IV.PROPOSING A SECURITY TECHNOLOGY

[4.1.1] RSA:

RSA is an algorithm for public-key cryptography, involves a public key and a nonpublic key. The overall public keys are regularly known to everybody and are utilized for scrambling messages. Messages encoded with the overall population key will exclusively be unscrambled abuse the particular key. Client information incorporate encryption before capacity, client verification methodology before capacity or recovery, and building secure channels for information transmission [3].RSA crypto framework understand the properties of the multiplicative Homomorphism encryption calculation and named after its creators.

[4.1.2]Key generation:

The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
- For security purposes, the integers p and q should be chosen at random, and should be similar in magnitude but differ in length by a few digits to make factoring harder.[2]Prime integers can be efficiently found using a primarily test.
2. Compute $n = pq$.
- n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
3. Compute $\lambda(n) = \text{lcm}(\lambda(p), \lambda(q)) = \text{lcm}(p-1, q-1)$, where λ is Carmichael's toting function. This value is kept private.
4 Choose an integer e such that $1 < e < \lambda(n)$ and $\gcd(e, \lambda(n)) = 1$; i.e., e and $\lambda(n)$ are co-prime.

Encrypting with public key{e,n}(c = me mod n)

1. Choose a clear text message call it m – in the form of a number less than n
2. Raise it to power e
3. Divide that by n call remainder c then your cipher text result is c

Decrypting with private key{d,n}(m = cd mod n)

1. Take cipher text c
2. Raise it to power d
3. Divide that by n call remainder r then your recovered result is r is identically the original clear text message m

[4.1.3] HOMOMORPHISM ENCRYPTION

Cloud consumer scrambles its information before sending to the Cloud supplier, but, each one time he need to deal with that will need to decode that information [2]. The customer will oblige giving the private key to the server to decode the information before to perform the counts obliged, which may impact the classifiedness of information put away in the Cloud..

[4.2.4] ENCRYPTION ALGORITHM

Algorithm: Encryption of given data

Procedure A: select the characters n(c);

B: converting the selected characters into ASCII values;

C: Forming the selected characters into m x m matrices; I.e. m x m > n(c);

D: dividing the m x m matrices into top, diagonal, lower matrices;

E: Read the values of each matrix and named as key K= k1, k2, k3;

F: Apply encryption method into matrix same order values i.e. to, diagonal, lower matrices;

G: Read column by column from the matrix and generates a key k4 (k4 is encrypted value);

[4.2.1] Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) may be a symmetric-key square figure calculation and U.S. government ordinary for secure and ordered encoding and unraveling. In December 2001, the National Institute of Standards (NIST) affirmed the AES as Federal experimental control Standards Publication (FIPS PUB) 197, which points out application of the Rijndael calculation to all or any touchy ordered information [2]. After a compelling assessment, the Rijndael configuration, made by two Belgian cryptographers, was the last decision [1].

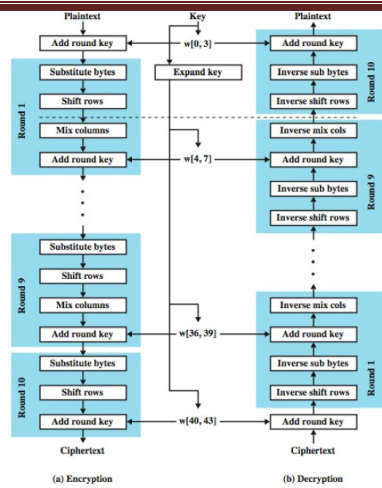

Fig 4: AES ALORITHM

[4.2.2] Symmetric-key algorithms:
Symmetric-key figuring's square measure those computations thatuse enduring key for every one encoding and riddle forming. Thusly the secret is unbroken puzzle [2]. The most basic kind of the encoding is that the good key encoding. Symmetric-key computations square measure those figuring's that use steady key for every one encoding and secret creating. Along these lines the riddle is unbroken secret. Perfect counts have the inclination of not overwhelming an unreasonable measure of figuring power and it works with high speed in encoding [1], [2].
The AES supplanted the DES with new and upgraded gimmicks:

- block encryption usage
- 128-bit bunch encryption with 128, 192 and 256-bit key lengths.
- 20-30 years for data security.

[4.3.1]Time Scheduling
Time scheduling is a collection of techniques used to develop and present *schedules* that show when work will be performed. General. The choice of tools and techniques used to develop a *time schedule* depends upon the level of detail available about the work that needs to be done. A schedule or a timetable, as a basic time-management tool, consists of a list of times at which possible tasks, events, or actions are intended to take place, or of a sequence of events in the chronological order in which such things are intended to take place. The process of creating a schedule - deciding how to order these tasks and how to commit resources between the variety of possible tasks is called scheduling, and a person responsible for making a particular schedule may be called a scheduler. Making and following schedules is an ancient human activity Some scenarios associate "this kind of planning" with learning "life skills".[4][5] Schedules are necessary, or at least useful, in situations where individuals need to know what time they must be at a specific location to receive a specific service, and where people need to accomplish a set of goals within a set time period.
The timing properties of a given task refer to the following items

- *Release time* (or *ready time*): Time at which the task is ready for processing.
- *Deadline*: Time by which execution of the task should be completed, after the task is released.
- *Minimum delay*: Minimum amount of time that must elapse before the execution of the task is started, after the task is released.
- *Maximum delay*: Maximum permitted amount of time that elapses before the execution of the task is started, after the task is released.
- *Worst case execution time*: Maximum time taken to complete the task, after the task is released. The worst case execution time is also referred to as the *worst case response time*.
- *Run time*: Time taken without interruption to complete the task, after the task is released.
- *Weight* (or *priority*): Relative urgency of the task.

[4.3.2]Standard Genetic Algorithm (SGA)
The Standard Genetic Algorithm is provided by schema. With them we can understand the Schema Theorem. It explains how crossover allows a genetic algorithm to zero in on an optimal solution. However, schema are inadequate in determining some characteristics of the population. Specifically, in determining the speed of population convergence, and the distribution of the population over time.
Using the proceeding notions, we now describe the seven steps in the Standard Genetic Algorithm:

1. Start with a population of n random individuals each with l-bit chromosomes.
2. Calculate the fitness f (x) of each individual.
3. Choose, based on fitness, two individuals and call them parents.
4. Remove the parents from the population.
5. Use a random process to determine

whether to perform crossover. If so, refer to the output of the crossover as the children. If not, simply refer to the parents as the children.

6. Mutate the children with probability p_m of mutation for each bit.
7. Put the two children into an empty set
8. called the new generation.
9. Return to Step 2 until the new generation contains n individuals. Delete one child at random if n is odd. Then replace the old population with the new generation. Return to Step 1.

V. CONCLUSION

We proposed a secure sharing of data using RSA and AES algorithm to maintain security within cloud server. KDM will be responsible for all key generation and key distribution process in our proposed scheme. The performance is evaluated and the results are obtained based on RSA key generation and AES encryption process. From the result, it is noticed that our proposed method will be applicable for sharing data in cloud securely. We use policy based access mechanism to provide security with the data in cloud and also to provide authentication. In future we can use multiple KDM to handle the data with different access policies to avoid insider attacks

VI. REFERANCE

1. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing." Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr.2010.https://doi.org/10.1145/1721654.1721672
2. Amazon, "Case Studies," http://aws.amazon.com/solutions/ casestudies/#backup, 2012.
3. Dropbox, http://www.dropbox.com, 2010.
4. Google Drive, http://www.drive.google.com, 2012
5. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, 2010.https://doi.org/10.1007/978-3-642-14992-4_13
6. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010.https://doi.org/10.1109/infcom.2010.5462173
7. W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and Efficient Access to Outsourced Data," Proc. ACM Workshop Cloud Computing Security (CCSW),Nov.2009.https://doi.org/10.1145/1655008.1655016
8. A. Yun, C. Shi, and Y. Kim, "On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage," Proc. ACM Workshop Cloud Computing Security (CCSW), Nov. 2009.https://doi.org/10.1145/1655008.1655017
9. R.L.Rivest, A.Shamir, and L.Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Communication of the ACM, Volume 21 No. 2, Feb. 1978. https://doi.org/10.1145/359340.359342
10. Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.