

Secured Data Migration Model Based On ACO Algorithm and RSA Encryption for Cloud Environment

Deepika, Amanpreet kaur

Department of Information Technology, Chandigarh Engineering College, Landran, Mohali, India

Abstract - Generally cloud computing requires either an application to be built especially for it, or for existing application to migrated to it. The main focus on migrate the application data with speedily and accurately. The series of technical, architectural and legal challenge created when migrating data to cloud which resolved by using following algorithms. Make the efforts to organize a set of migration schemes and list of reusable solution in form of packets, than connected it in application of data migration. In last, methodology of data migration and practically how it can be used defined.

Keywords - Cloud Computing; Data Migration; RSA Encryption; ACO Algorithm.

I. INTRODUCTION

A. CLOUD COMPUTING

In general term cloud computing is a process of dispatching of organizes services atop the internet. Cloud computing due to their reliability also beneficial for businesses and end users. The economic computing model of cloud computing consist of different types of services [1] such as: 1) Infrastructure as a Service (IaaS), customers have infrastructure where migrate the service; 2) Platform as a Service (PaaS), customers have platform where build up or run applications; and finally 3) Software as a Service (SaaS), customers have a software to consume the services. [1]. The cloud computing have following four deployment prototypes have been identified on basis of services and user of cloud: Private cloud: The infrastructure of cloud prepared, maintain and operate for private organization; Public cloud: the substructure of cloud is obtainable to the public on a commercial basis by a cloud service provider; Hybrid cloud: the combination of private and public clouds that provision the requirement to retain some information in an organization; Community cloud: the infrastructure of cloud distributed between limited organizations. [17]

B. DATA MIGRATION

In data migration process the transfer of application data from a cloud server or cloud servers to the new environment. In business deployment application that data migration works as sub activity. The vital role performs by data migration in ensuring business continuity. The substantial focus and attention, and discipline, required like: (1) Due to the data migration process no data loss, (2) Also data not polluted and

(3) Data changed is updated by only default rules [7]. Data migration is a process of resettling between storage types, formats and computers systems [5]. Basically it is programmatically preformed to achieve automated migration, which freeing up human resource from tedious tasks. Data migration process has different phases to migrate the data from one server to another: planning, profiling, Cleaning, post production and pre-production [3].

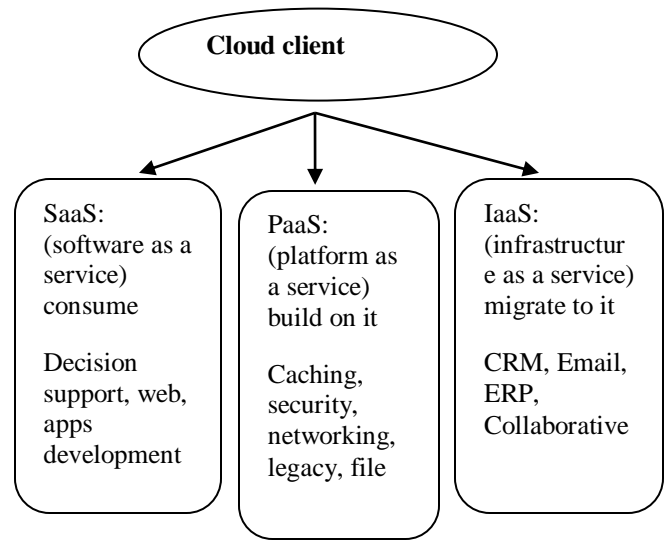


Fig 1: cloud client and their services

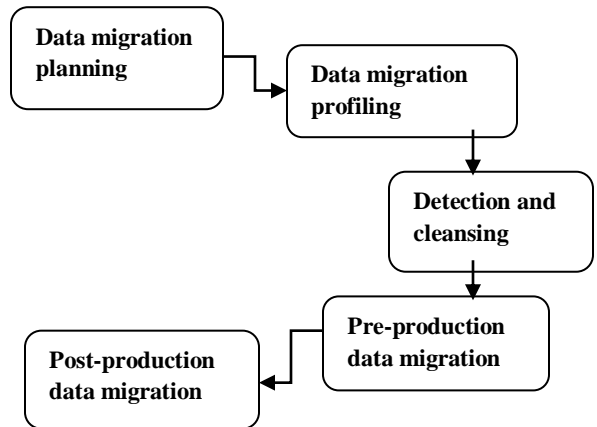


Fig 2: Phases of data migration process

These are phase of data migration:

- **Data migration planning:** define scope and requirement of project; assess current and target environment; develop the data migration plan
- **Data migration profiling:** identify source system; define business logic; analyze legacy system data dictionary & definition.
- **Detection and cleansing:** identify potential bad /inconsistent data; perform cleansing of identify exception.
- **Pre-production data migration :**synchronize the data between legacy system and new system
- **Post-production data migration :** migration of data legacy system to new system; transform of data

II. CHARACTERISTICS OF DATA MIGRATION

Basically, the procedure of data migration is transferring data from one server to additional server while changing the storage, database or application of cloud servers. In position to the Extract Transform-Load process, data migration always requires or transfers to an entirely new system. Examples include: Relocation to or from hardware platform; upgrading a database or travelling to new software; or company mergers when the parallel systems in the two businesses need to be merged into one. [12] The data migration is preformed due to following:

1. Combine the concerns of two servers into a new server[11]
2. Transmission one server to another server.
3. Create a backup of system due security point of view

One significant step to take is to make sure that the client appreciates the importance of the scope of presence it and the risks that may occur due to the lack of it. With the benefits, it's easy for the client to view the scopes as time consuming and redundant.

III. OPTIMIZATION TECHNIQUES FOR DATA MIGRATION

- **ANT Colony Optimization (ACO):** ACO will be a streamlining procedure dependent upon computerized reasoning frameworks which impact or motivate by *nature of real ant colonies*. Also which may be utilized discrete streamlining should fathom issues.
- **Genetic Algorithm Optimization:** Those streamlining methodology dependent upon Taking in machine which make perfect starting with allegory for improvement. Those methodology executes by Taking in machine of a populace done which personalities quell Eventually Tom's perusing chromosomes What's more a set from claiming character

strings base-4 chromosomes which comparable with human DNA.

- **BEE Colony Optimization:** The searching optimization process which based on population developed in 2005. The bee colony optimization follows food foraging technique of honey bee colonies. Previously, real adaptation the calculation performs combinational streamlining such as neighborhood What's more worldwide looking use together.
- **Particle Swarm Optimization (PSO):** The PSO will be a computational technique that optimizes an issue by iteratively attempting on enhances a hopeful result for respects with. A provided for measures about nature. They tackled the issue utilizing straightforward scientific formulae's. In the molecule position what's more speed.

IV. SECURITY TECHNIQUES FOR DATA MIGRATION

1. **RSA Encryption:** The encryption method presented toward ron Rivest, Adi Shamir, Furthermore leonard Adleman that the reason called it RSA encryption. On RSA utilized cryptographic calculation which replace ability national department of guidelines (NBS) calculation due to a greater amount security. Basically, RSA usage relies upon further two strategies public-key cryptosystem further more advanced marks. A number a considerable length of time in the recent past Diffie. Also hellman distributed their work, At not actualize all the it. Really RSA take clue from publish worth of effort Furthermore execute it previously, 1978.

RSA implemented depend upon two techniques:

a. Public-key encryption: In this technique, in front of channelize genuine message through another secure channel necessity. A messenger on beneficiary conveys way. RSA bring you quit offering on that one encryption keys which is general population and one unscrambling keys need aid private, thereabouts message just interpret toward who have straight unscrambling enter. Encryption Also unscrambling keys gatherings give on client something like that effectively message get it.

b. Digital signatures: In which worth of effort once confirmation about message may be exchange toward first sender. Those sender utilization unscrambling enter to confirmation What's more advanced signature checked Eventually Tom's perusing who utilize the relating general population encryption way. Marks can't be fashioned.

2. **Public key Cryptography:** Public-key cryptography is a security procedure which likewise called two-key or deviated cryptography since done which utilization of two keys: particular case public-key, which is nearby what's more utilized Toward Everybody and different private-key which may be utilized by the individuals have unscrambling key.

Public-Key calculations built two keys qualities which may be computationally infeasible to Figure unscrambling magic & encryption enter computationally not difficult to encrypt/decrypt messages when key learning over whichever fact that utilized to encryption alternately unscrambling.

3. Triple DES: triple des might have been outlined to displace the first information encryption standard (DES) algorithm, which hackers inevitably taken in on rout with relative simplicity. During person time, triple des might have been those recommended standard and the vast majority generally utilized symmetric calculation in the industry. Triple des utilization three singular keys for 56 odds each. The downright magic period includes dependent upon 168 bits, Anyway masters might argue that 112-bits. On magic quality is additional in it. Notwithstanding gradually being phased out, triple des at present manages should aggravate a trustworthy equipment encryption result to money related administrations and different commercial enterprises

AES: Those advanced encryption standard (AES) may be those algorithm trusted similarly as those standard toward the u. In spite of it may be greatly productive clinched alongside 128-bit form, AES likewise utilization keys of 192 Furthermore 256 odds to overwhelming obligation encryption purposes. AES is generally acknowledged impenetrable with at attacks, for the exemption about beast force, which endeavours will interpret messages utilizing at could reasonably be expected combinations in the 128, 192, alternately 256-bit. Still, security masters trust that AES will in the end make hailed the accepted standard to encrypting information in the private division.

V. RELATED WORKS

Shen, et.al, [1] depict information movement security issue in distinctive clouds. Utilization Emulating steps viewing security: 1st, recognize dangers throughout the methodology of relocation. Over next instrument actualized which taking care of those threats, the point when information could make migrated from one server will in turn you quit offering on that one. Done last, model might be configuration and actualize all rely on Hadoop dispersed record framework (HDFS). To which no from claiming test arrangement assess to model execution. The security from claiming information relocation might a chance to be figure out by accompanying parameters SSL negotiation, movement ticket outline Also square encryption in dispersed record framework Furthermore bunch parallel registering.

In [2] **Chadi Kari, et.al,** Accepted that know hub from claiming capacity could detract special case information exchange at once. Each capacity hub handles different assignments simultaneously and because of this decrease

previously, aggregate relocation chance. In this paper, recognizing the arranged information movement problematic, the place expect that every stockpiling hub v need separate exchange demand CV, which characterizes know what number of immediate transfers, might handle. Real concentrate on create and execute calculations should minimize duration of the time of the information movement procedure.

As discussion **Yunpeng Chai, et.al, [3]** characterizes most recent Vitality productive method called unequivocal vitality sparing plate cooling alternately EESDC. EESDC techno babble fundamentally diminishes information relocation due to two reasons. 1st, a set for plates examined should unequivocal vitality sparing plates might have been clearly settled as stated by transient framework load. Subsequent, the migrated information to EESDC specifically back on extending the unmoving pulley chance about EESD with reservation more vitality proficiently. Therefore, the EESDC strategy is helpful will sparing more vitality toward rapidly accomplishing Vitality productive information layouts without excess information migrations. Those instruments for EESDC to A recreated circle framework would verify against a model framework mechanical toward our EESDC.

Hui Liu et.al, [4] ponder those conveyance model about cloud registering aspects. For the information capacity plan headway for SaaS, every last bit tenants' information necessity on a chance to be voyaged under the new information diagram in the recent past it turns into agent to guarantee the integument of the tenants' information. However, relocation transform may be composite Also carries overhead workload. On paper, suggest advancement of metadata engineering organization. Smooth mapping starting with old information diagram to new information plan. **Yanling Du et al. [5]** describe hybrid cloud storage with features like high performance, high retreat of private cloud and the large capacity of public cloud. . For measurable expressing of the ongoing property, compassion, decentralization Also information get high temperature from claiming oceanic data, the place accepted the model about marine for information movement the middle of separate mixture clouds. Information relocation technique might have been enhanced impermanent for avoiding limitation of the universal information movement methodology which real made as stated by the information entry **Pawan Nahar et.al, [6]** characterize information movement about dynamic cloud motor. Build information rate day toward day, In this way examination enormous information is necessary which will be challenge, That's reason the reason association hunt cloud capacity Hosting secondary proficient stockpiling foundation set up will help secondary scale operation, without reduction of information. IBM bring dynamic cloud engine, for features about enhances the methodology from claiming information movement Eventually Tom's perusing caching information for

around the world over accessible it with zero down time generally.

In [7] **Koongwahyan, et.al**, Information relocation biological community for huge information is those set for intelligent transform for production, hones Furthermore aggregate information earth from one area capacity medium convert in turn. The polishes took care of toward standards Also controls with full learning about helter shelter precision Furthermore consistency.

Jianzhe Tai, et al. [8] used live data migration for decrease service level agreements (SLA). Over which enormous repudiate may be sets information of store procedure and inquiry expansive scale information. Done which multi-tiered stockpiling framework is utilized Likewise another approach to programmed information movement, the place energetic information movement supported with esteemed SLA's. LMT's upgrade Normal I/O reaction time, I/O violation time and I/O violation proportion with minor corruption a head execution from claiming exceedingly necessity requisitions.

Cui Shuo et al. in 2014 [9] depict the stockpiling for impostor information which relocation transform help benefits of the business benefits, information stockpiling security, information integument necessities, same time also research on answer engineering for monstrous information which dependent upon stockpiling square the place non concurrent relocation strategy utilized to everyone over profits .**Steve Strauch, et al., 2014[16]** said that cloud registering required for particularly Fabricate application, and other for now introduce requisition on migrated to it. Migrating information of the cloud server aggravated arrangement from claiming technical, structural and legitimate tests. Over which set of movement plan Furthermore associate it with a rundown about reusable result over design structure for information relocation provision.

VI. PROBLEM FORMULATIONS

During the process of data transfer from one cloud server to another has data loss and data corruption risk. A source server of a cloud has a large amount of data so it's difficult task to transfer the data accurately in less time to destination server. In such a case a tool is required through which transfer of the data from one cloud to another. Migration of the data is quite difficult task because every cloud server has its own protocol service to work. Some mediator protocol service would be required which can understand both cloud servers' protocols [16]. In proposed work, signify a mediator protocol service as bridge which communicates with both the cloud servers and successfully data migrate from one cloud server as source to another cloud server as a destination. Optimize migration of data using ANT Colony Optimization (ACO) algorithm which also makes fast transmission. Add RSA encryption to maintain data security and accuracy [17].

VII. OBJECTIVES

Our objectives includes the following

- To implement the data migration framework in cloud environment which work as a mediator protocol.
- To optimize the performance of migration using ACO algorithm in terms of accuracy based on error rate, throughput related to transfer rate, error and probability check by secure transmission.
- To evaluate the above performance parameters and compare the results with previous reusable pattern techniques used earlier.

VIII. PROPOSED MODEL

The process of data migration over cloud environment need to be follow different rules of two servers in which data transfer, Because every server has their own different protocols. Firstly, migration of data started by detection of data which migrated than make their schemas. Classification of tables and entities, re-organize the types and make structure of columns use for pattern. ACO Algorithm apply on bit pattern for optimize the migration so that migration of data one cloud to another take less-time. When all bit patterns optimize than apply RSA encryption to bit stream section so data transfer one cloud to another securely and accurately. After implement ACO Algorithm and RSA encryption on bit pattern generate migration request. Using handshaking process, Request send by one cloud server and another cloud send back acknowledge. In between protocol active in both server and make common bridge to joint both cloud servers. For sending packets launch an optimized path by ACO. At the end launch migration process. Data accurately, securely and timely transfer than stop the process

IX. CONCLUSIONS

The process of data migration transfer data from one cloud server to another server. Process seems to be very simple and easy but it is not. Because every cloud server have their different protocols and rules. At time of data transmission possibility of data loss, data theft and transmission take more time. These series of technical, architectural and legal challenge occur. To resolve these challenges use different techniques and algorithms. Techniques are like: adjoin two different protocol clouds server using mediator protocol in between as bridge. ACO Algorithm used for optimization data so take less time in transmission. RSA Encryption applies on bit stream so securely and accurately data migrating one cloud server to another. So that procedure makes data migration process accurate, secure and fast

X. REFERENCES

- [1]. Shen, Qingni, et al. "SecDM: Securing data migration between cloud storage systems." Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on. IEEE, 2011.
- [2]. Kari, Chadi, Yoo-Ah Kim, and Alexander Russell. "Data migration in heterogeneous storage systems." Distributed Computing Systems (ICDCS), 2011 31st International Conference on. IEEE, 2011.
- [3]. Chai, Yunpeng, et al. "Efficient data migration to conserve energy in streaming media storage systems." Parallel and Distributed Systems, IEEE Transactions on 23.11 (2012): 2081-2093.
- [4]. Liu, Hui, and Shengqi Wu. "Data storage schema upgrade via metadata evolution in SaaS." Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference on. IEEE, 2012.
- [5]. Du, Yanling, et al. "Study of migration model based on the massive marine data hybrid cloud storage." Agro-Geoinformatics(Agro-Geoinformatics), 2012 First International Conference on. IEEE, 2012.
- [6]. Nahar, Pawan, Abhidnya Joshi, and Alexander Saupp. "Data migration using active cloud engine." Cloud Computing in Emerging Markets (CEM), 2012 IEEE International Conference on. IEEE, 2012.
- [7]. KoongWah Yan et al., "Data Migration Ecosystem for Big Data", 978-1-4799-0786-1/13/\$31.00 ©2013 IEEE
- [8]. Tai, Jianzhe, et al. "Live data migration for reducing sla violations in multi-tiered storage systems." Cloud Engineering (IC2E), 2014 IEEE International Conference on. IEEE, 2014.
- [9]. Shuo, Cui, et al. "Research and application on mass data storage replication technology." Electricity Distribution (CICED), 2014 China International Conference on. IEEE, 2014. Miyamoto, Naoyuki, Kenichi Higuchi, and Takao Tsuji. "Incremental Data Migration for Multi-database Systems Based on MySQL with Spider Storage Engine." Advanced Applied Informatics (IIAIAA), 2014 IIAI 3rd International Conference on. IEEE, 2014.
- [10]. Karnitis, Girts, and Guntis Arnicans. "Migration of Relational Database to Document-Oriented Database: Structure Denormalization and Data Transformation." Computational Intelligence, Communication Systems and Networks (CICSyN), 2015 7th International Conference on. IEEE, 2015.
- [11]. Miyamoto, Naoyuki, Kenichi Higuchi, and Takao Tsuji. "Incremental Data Migration for Multi-database Systems Based on MySQL with Spider Storage Engine." Advanced Applied Informatics (IIAIAA), 2014 IIAI 3rd International Conference on. IEEE, 2014.
- [12]. Ou, Jiaxin, et al. "EDM: An endurance-aware data migration scheme for load balancing in SSD storage clusters." Parallel and Distributed Processing Symposium, 2014 IEEE 28th International. IEEE, 2014.
- [13]. Tan, Zhenyu, et al. "ALDM: Adaptive Loading Data Migration in Distributed File Systems." Magnetics, IEEE Transactions on 49.6 (2013): 2645-2652.
- [14]. Wu, Suzhen, Hong Jiang, and Bo Mao. "Proactive Data Migration for Improved Storage Availability in Large-Scale Data Centers." Computers, IEEE Transactions on 64.9 (2015): 2637-2651.

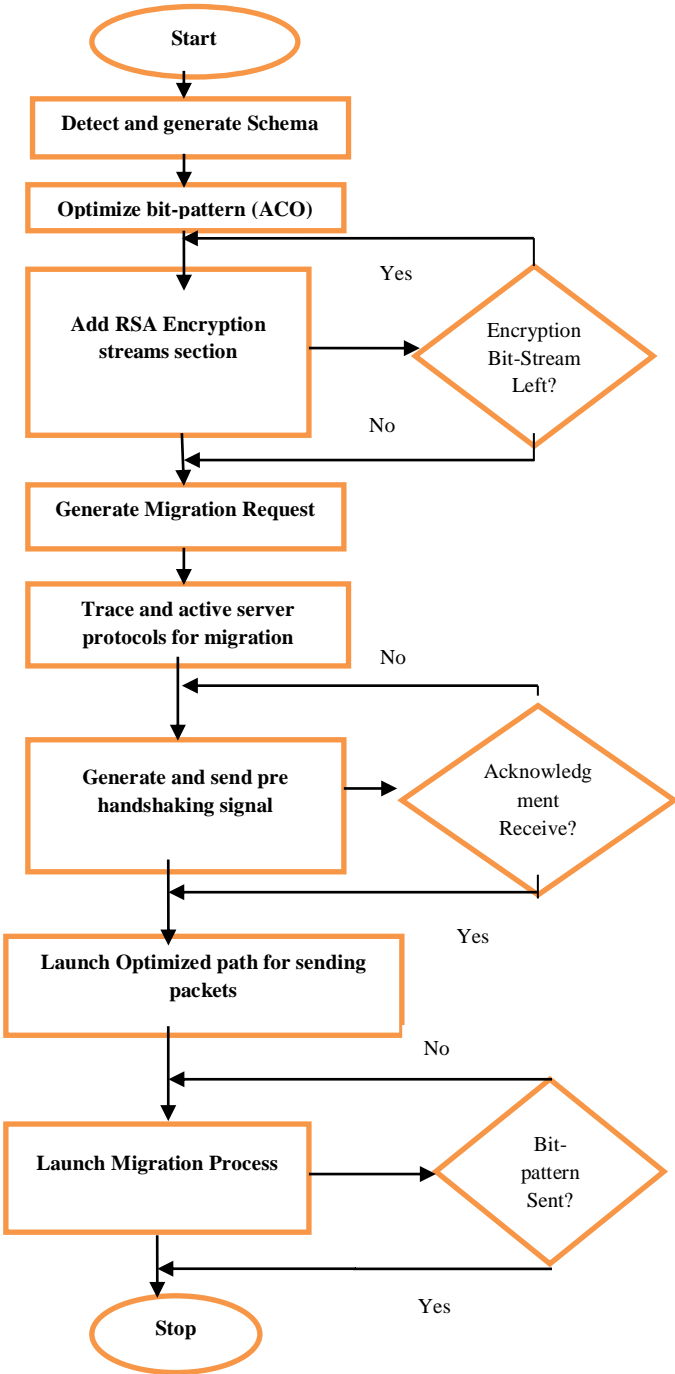


Fig 3: flow chart

- [15]. Wu, Chentao, et al. "Sdm: A stripe-based data migration scheme to improve the scalability of raid-6." Cluster Computing (CLUSTER), 2012 IEEE International Conference on.IEEE, 2012.
- [16]. Steve Strauch, VasiliosAndrikopoulos, Thomas Bachmann and Frank leymann migrating application data to the cloud using cloud data patterns 2014 IEEE ROMAN: Issued 9, June 2014.paris France computer science and technologies.

- [17]. Amanpreet kaur, Dheerendra Singh define exploring data security issue and scrutinizing them in cloud computing environment, IJITKM volume 8 number 1 June - dec 2014
- [18]. Amanpreet kaur, Dheerendra Singh ,Kanika minhas ,”mitigation of high rate shrew DDOS attack ’international journal of modern computer science :issued 3, October ,2015