|| Volume 2 ||Issue 10 ||MAY 2017||ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

A Survey on ACO and Cryptography Techniques for Cloud Computing Security and Privacy

Ms. P. M. Rokade[1] , Dr. S.S.Lomte[2]
Research Student, Dr. B.A.M.U Aurangabad, Maharashtra, India[1].
Rokade.punam@gmail.com
Principal, V.D.F. School of Eng. & Technology, Latur, Maharashtra, India[2].
santoshlomte@hotmail.com

***Abstract*— Cloud computing is a technology evolution of adoption of virtualization, service oriented architecture and utility computing over the internet including applications, platform and services. Cloud security and privacy is a biggest concern about cloud computing, because the user do not know where the data is stored, what position the data and which servers are processing the data. Also what network are transmitting the data because of the flexibility and scalability of cloud system. This paper introduced the cloud architecture and its building blocks and service models. Also different technologies used for cloud system security in different applications in order to improve and enhancing the cloud system security and performance. Mainly, we focus on the discussion of Ant Colony Optimization technique used by different authors.**

***Keywords*—**cloud security, ant colony algorithm, genetic algorithm, cryptography, stenography.

I INTRODUCTION

Cloud computing is a combination of technology, platform that hosting and storage service on the internet [1], that provides shared computer processing resources and data to computers and other devices on demand [*2,3]. It is* simply means, the Internet computing. Generally the internet is seen as collection of clouds; thus the word cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. In this environment user need not own the infrastructure for various computing services. It can deploy, allocate or reallocate resources dynamically with an ability to continuous monitor their performance. Thus, the main aim of cloud computing is to provide scalable and inexpensive on-demand computing infrastructure with good quality of service levels. It enables users to access resources online through the internet via the browser and deployed on millions of machines, from anywhere at any time without worrying about technical/physical management and maintenance issues of the original resources. Besides, Resources of cloud computing are dynamic and scalable [4].

Cloud computing is an emerging trend to deploy and maintain software and is being adapted by the industry such as Google, IBM, Microsoft, and Amazon. It can be applied to solve problems in many domains of Information Technology like GIS(Geographical Information Systems), Scientific Research, e-Governance Systems, Decision Support System, ERP, Web Application Development, Mobile Technology, etc.
The use of word "cloud" makes reference to the two essential concepts:

Abstraction: Cloud computing abstracts the details of system implementation from users and developers. Applications are run on unspecified physical systems, data stores at unknown locations, systems administration is outsourced to others, and access by users is ubiquitous.

Virtualization: Cloud computing virtualizes systems by pooling and sharing resources. The centralized infrastructures are used for systems and storage when needed. The costs are assessed on a metered basis, multi-tenancy is enabled, and resources are scalable with agility [1].

II CLOUD COMPUTING BUILDING BLOCKS

There are two types of cloud models as deployment models and service models described below:

A. Deployment Models:

This refers to the location and management of the cloud's infrastructure, define purpose of the cloud and the nature of how the cloud is located. The NIST (National Institute of standard and technology) defines four types of development models as: Public cloud, Private cloud, Community cloud and Hybrid cloud.

1. Public Cloud:

This model allows users to access the cloud infrastructure via interfaces using web browsers and typically based on pay-per-use model [5, 6]. It is available to general public or a large industry group [7,] via a multi-tenant model on a self-service basis delivered over the internet. It is owned by a large organisations . Amazon's EC2,Google's AppEngine and Microsoft's Azure [Ramasami S.March2012]. These services may be free or not [Raj Kumar] and are less secure than other

models because it places an additional observation to ensure all applications and data accessed on the public cloud are not subjected to malicious attacks [6].

2. Private Cloud:

In this model the cloud infrastructure is operated for one organization and may be managed by the organization or a third party, and may exist on premise or off premise. The scalable resources and virtual applications are pooled together and make available to share and use for cloud users. It is easy to align with security, compliance, and regulatory requirements, and provides more enterprise control over development and use [6]. It is more secure [7] because of its specified internal exposure. The best example of private cloud is Eucalyptus Systems [5].

3. Community Cloud:

In this model, cloud infrastructure could be shared by several organizations and supports a specific community or interest group that has shared concerns such as mission security, requirements, and policy and compliance considerations. The goal of a community cloud is to have participating organizations realize the benefits of a public cloud such as multi-tenancy and a pay-as-you-go billing structure. It has added level of privacy, security and policy compliance, and usually associated with a private cloud. It either on-premise or off-premise, and can be governed by participating organizations or by a third-party managed service provider [5, 6]. It may exist locally or remotely. These clouds are normally based on an agreement between related business organizations such as banking or educational organizations. E.g. Facebook.

4. Hybrid Cloud:

It is a composition of two or more clouds (private, public or community cloud) [4], at least one private cloud and one public cloud. This cloud is typically offered in one of two ways: a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms, which only accessible by certified staff and protected by firewalls from outside accessing and external users of public cloud can access to it. Thus, it provides more secure control of data and applications, and allows various parties to access information through Internet [6].Amazon Web Services (AWS) is an example of a Hybrid Cloud [5].

B. Service Models:

We can think of the cloud as the boundary between where a client's network, management, and responsibilities ends and the cloud service provider's begins [1]. Cloud computing services themselves fall into three major categories:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

1. Software as a service (SAAS):

It simply means delivering software applications by Application Service Provider (ASP) over the Internet. The software running on the provider's cloud infrastructure, delivered to multiple clients on demand via a thin client e.g. browser over the Internet. So the customer get rid of installing and operating application on own computer and eliminate tremendous software maintenance load, continuing operation, safeguarding and support.SaaS vendor has responsibility for deploying and managing the IT infrastructure (servers, operating system software, databases, data center space, network access, power and cooling, etc) and processes (infrastructure patches/upgrades, application patches/upgrades, backups, etc.) required to run and manage the full solution.

Two types of servers are used by SaaS: Main Consistence Server (MCS) and Domain Consistence Server (DCS). Cache coherence is achieved by the cooperation between MCS and DCS. In SaaS, if the MCS is damaged, or compromised, the control over the cloud environment is lost. Hence securing the MCS is of great importance. Google Docs and Salesforce.com CRM are examples ofSaaS[5, 8].

2. Platform as a Service (PaaS):

The aim of this model is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure to develop, test and deploy applications on the provider's platform (API, storage and infrastructure) with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure including network, servers, operating systems and storage, but he controls deployed applications and, possibly, their configurations. Force.com, Google App Engine and Microsoft Azure are examples of PaaS [5, 8].

3. Infrastructure as a Service (IaaS):

It refers to the sharing hardware resources for service execution using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. IaaS runs on a tenancy model, which employs a usage-based payment approach allowing users to pay for resources only those they actually use [8].Examples of IaaS are Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid [5].

III CHARACTERISTICS OF CLOUD COMPUTING

Cloud computing exhibit five essential characteristics as below:

- ***On-demand self-service:***A client can use resources without the interaction with cloud service provider.

- ***Access to resources:*** Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms like operating systems, laptops, mobile phones, and PDA [7].
- ***Resource pooling:*** The provider's computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned as needed to supports multi-tenant usage. In this pooling concept the idea of abstraction that hides the location of resources such as virtual machines, processing, memory, storage, and networking bandwidth and connectivity.
- ***Rapid elasticity:*** Resources can be rapidly and elastically provisioned to quickly scale out and rapidly released to quickly scale in.
- ***Measured service:*** The use of cloud system resources is measured, audited, and reported to the customer based on a metered system [1].

IV CLOUD SECURITY

The biggest concerns about cloud computing are security and privacy [9, 4] because cloud computing and web services run on a network structure so they are open to network type attacks. There are some traditional security problems like security vulnerabilities; virus and hack attack can lead more serious results. Hackers and malicious intruder may hack into cloud accounts and steal sensitive data stored in cloud systems. It is discomfort too many to put your data, run your software at someone else's hard disk using someone else's CPU, so the cloud system must protect the resources carefully.

One of the attacks is distributed denial of service attacks. If a user could hijack a server then the hacker could stop the web services from functioning and demand a ransom to put the services back online. To stop these attacks the use of cookies and limiting users connected to a server all help stop a DDOS attack. Another attack is the man in the middle attack because of incorrect configuration of secure sockets layer (SSL), so the client and server authentication may not behave as expected therefore leading to man in the middle attacks. The security issues such as data loss, phishing, and botnet (running remotely on a collection of machines) poses serious threats to organization's data and software. The Data loss, Leakage of Data, Client's trust, User's Authentication, Malicious users handling, Wrong usage of Cloud computing and its services are the top security concerns of cloud computing.

Figure 1. Shows the network architecture for cloud data storage. It contains three parts as Users, Cloud Service Provider (CSP) and Third Party Auditor (TPA).

V ANT COLONY OPTIMIZATION ALGORITHM

Ant Colony Optimization (ACO) algorithm was initially proposed by Macro Dorigo in 1992 to solve real world complex problems such as the travelling salesman problem, data mining, etc. It is a probabilistic technique for solving computational problems which can be reduced to finding good paths through graphs. As in the natural world, ants of some species wander randomly, and upon finding food return to their colony while laying down pheromone trails. If other ants find such a path, they are likely not to keep travelling at random, but instead to follow the trail, returning and reinforcing it if they eventually find food.

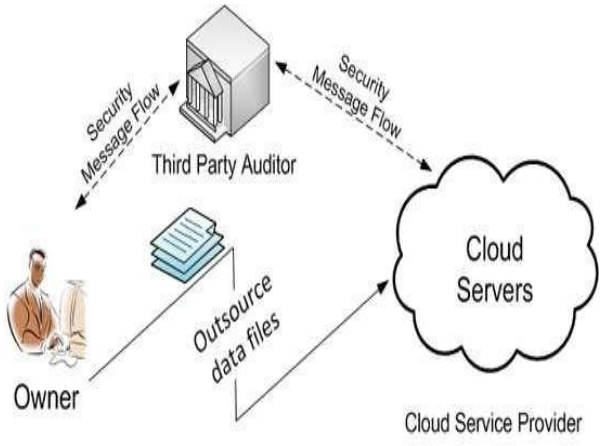

Figure 1 Cloud Data Storage Architecture

ACO algorithms solve a problem based on the following concept:

- Each path followed by an ant is associated with a candidate solution for a given problem.
- When an ant follows a path, it drops varying amount of pheromone on that path in proportion with the quality of the corresponding candidate solution for the target problem.
- Path with a larger amount of pheromone will have a greater probability to be chosen to follow by other ants. The process is thus characterized by a positive feedback loop, where the probability with which an ant chooses a path increases with the number of ants that previously chose the same path.

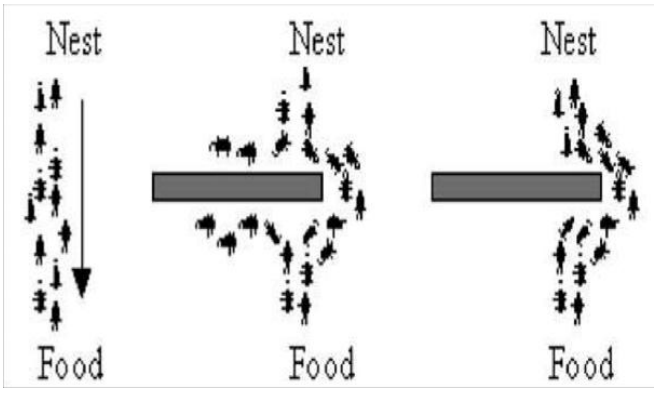

Figure 2 How ants find flood from the nest

ACO makes probabilistic decision in terms of the artificial pheromone trails and the local heuristic information. This allows ACO to explore larger number of solutions than

greedy heuristics. Another characteristic of the ACO algorithm is the pheromone trail evaporation, which is a process that leads to decreasing the pheromone trail intensity over time. Pheromone evaporation helps in avoiding rapid convergence of the algorithm towards a sub-optimal region.

VI LITERATRE SURVEY

The implementation approaches for Ant Colony Optimization algorithms was illustrated by the following research papers. The research papers are studied from the year 2012 onwards.

Hitesh Hasija and Rahul Katarya, incorporate a method for efficient code generation based on the frequency of occurrences of alphabets into the document. It used relative occurrence matrix and ant colony optimization with roulette wheel selection algorithm and suitable values of constants for that. Plaintext alphabets are usually coded with ASCII values during transmission of documents over the network, and getting those alphabets back from ASCII values is very easy for intruders. Hence, assigning ASCII values is not secure. If alphabets having large ASCII values appears frequently in document, then large number of bits are required for alphabets transmission. So, reassigning of code is necessary to achieve compression.

K.Sriprasadh and M.Prakash Kumar introduced different data retrieval techniques from largest database over cloud servers. It can be retrieved through an optimization technique like Boolean Symmetric Searchable Encryption, Secure Ranked Keyword Search over Encrypted Data and Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data, Over Encrypted Data in Cloud Computing, etc. Here, they used Ant Hill optimization technique to solve this problem. This method is designed for combinatorial problems and best known heuristics for data retrieval. It is shown that the ant colony method performs with little variability over problem instance.

Dilpreet kaur and Dr.P.S Mundra used Ant colony optimization technique to find the shortest path finding algorithm in spite of GPS or any other method. It Forms a zigzag track generated randomly by the algorithm. The aim of authors is to compare the time and accuracy to build a chat with old algorithms and used for searching and scanning the shortest path in between two points selected randomly by the user. This algorithm is basically designed for edge detection but here is implemented to find the path through hurdles.

Sri Hari Krishna Vuppalapati and Anurag K. Srivastava have developed and implemented reconfiguration of shipboard power system (SPS) using ACO in MATLAB.SPS supplies energy to sophisticated systems of weapons, navigation, services and communication. Electric energy delivery may be interrupted to critical loads due to battle damage or faults. Reconfiguration of electrical network in the SPS is necessary, to either restore the service to all the possible loads or to meet some of the operational requirements of the naval ship. Graph theory has been applied to represent SPS electrical network to simplify the mathematical formulation to be used by ACO. Here, developed technique has been applied to an eight bus and thirteen bus representative shipboard power system model to reconfigure, while maximizing the load magnitude, or load priority, or load magnitude with priority.

Authors obtained satisfactory results for both test cases. The mathematical problems were formulated to maximize the objective function considering (i) load magnitude only (ii) load priority only (iii) both load magnitude and load priority. Developed ant colony optimization technique has been tested for two test cases under several fault scenarios. Simulation results obtained are satisfactory and proposed method can be easily extended for application to bigger distributed power system.

Sudip Kumar Sahana proposed Modified Ant Colony Optimization (MACO) algorithm which is based on Ant Colony System (ACS) with some modification in the configuration of starting movement and in local updation technique to overcome the basic limitations of ACS such as poor initialization and slow convergence rate. It is shown that MACO gives better convergence speed and consumes less time than conventional ACS. The concept of multicasting is useful for many applications like the transfer of the audio, video and text of a live lecture to a set of distributed lecture participants, teleconferencing application that is shared among many distributed participants, multiplayer games. The developed modification could be applied to other applications like Vehicle Routing Problem, Job Shop Scheduling Problem, Constraint Satisfaction Problems, etc.

Gang Liu, Hua Wang and Hong Zhang proposed an algorithm of Overlay Backbone Multicast Routing in Content Delivery Networks. They frame the problem in their work as a constrained spanning tree problem which will prove is NP-hard. Live video streaming is a killer application in content delivery networks (CDNs), and is both resource-intensive and latency-sensitive. The large-scale live video-streaming in CDNs is a challenging to build stable, efficient and cost effective infrastructure. The Akamai commercial CDNs Technologies adapt the infrastructure based overlay multicast mechanism to support live video streaming broadcast. This approach relies on a set of geographically distributed and dedicated CDN servers with large processing power and high fan-out capability. This streaming technology largely benefits from the wide reach and large capacity of Akamai platform, consists of over 20,000 servers distributed in more than 70 countries. By using this algorithm, the access bandwidth demand can be reduced and simulation experiments confirm that the distributed algorithm performs well in seeking, convergence speed and adaptability scale.

Vasily A. Maistrenko and **Leonov V. Alexey** proposed different methods of routing in FANET (Flying Ad Hoc Network). For effective usage of protocol based on ant colony algorithm. It is complex task because of dynamically changing topology, 3-D movement and high mobility nodes. These are similar to mobile peer-to-peer networks MANET (Mobile Ad Hoc Network) and vehicle peer-to-peer networks VANET (Vehicular Ad Hoc Network) based on unmanned aerial vehicles (UAV). These can used to perform observation, monitoring, coordinate vehicle traffic effectively in order to prevent vehicle crash, etc. Intelligent routing methods in MANETs based on ant algorithm is presented in review.

In done experimental research there were analyzed AODV, DSDV, DSR and AntHocNet routing protocols. AntHocNet protocol exceeds AODV and DSDV protocols in packet delivery, average end-to-end delay, especially in conditions of node plenty. This is due to AODV and DSDV low working in conditions of high mobility of nodes. According to experiment DSR and AntHocNet protocols are more preferable for net with high mobility of nodes. AntHocNet is less effective because of high costs for routing service information transfer. In this case the weaknesses of one algorithm are neutralized by the advantages of another one. The higher convergence rate is reached and is followed by increasing network performance and decreasing requirements to hardware resources of nodes.

Ashwini Digambar proposed feature optimization based multi-label data categorization, based on ANTS algorithm and cluster mapping technique. In multi-label data categorization, feature optimization and feature selection plays an important role as it share a common class and classification process suffered a problem of selection. The feature optimization and classification of some standard dataset are done using ACO and cluster mapping respectively. All these data obtained from UCI machine learning centre. The implementation is done in MATLAB software. The experimental result shows that better classification result instead of RSVM and MLKNN algorithm.

The public key cryptography algorithms implementation approaches was clarified by the following research papers.The first paper was named Matrix based Asymmetric Bulk Encryption Algorithm and was written by Mukesh Kumar Singh of Texas Instruments. Also Farshid Delgosha and Farcmarz Fekri and is entitled Public Key Cryptography using Paraunity Matrices.

Rajat Jhingran presented Genetic Algorithm (GA) application in cryptography field for e-security application with pseudorandom sequence to encrypt and decrypt data stream. Basically, GA is a search based on the mechanics of natural selection and natural genetics. This paper describes the basics of genetic algorithm, cryptography with the help of some algorithms to keep the security of images based on crossover, mutation, and selection etc. the image encryption algorithms try to convert an image to another image that is hard to understand.

Karun Handa and Uma Singh, performed two basic processes of encryption and steganography for data security in cloud computing using java. In this method, images produced after steganography has been constructed so that it is not possible to differentiate between original and stego images and hence not possible to detect the presence of data. They used images for the testing purpose are of 1920*1080 pixels. The bits per pixel is 24bpp. The technique of image compression would be added to improve storage in future.

A.Mahesh Babu, G.A. Ramachandra and M.Suresh Babu build the cloud systems prototype based on steganography for security improvement using encryption and stenography. The system that can encrypt secret message and personal information embed it into an image file by using a new morphing based steganographic technique. The dynamically generated morphing image covers the massage which wants to hide, and there are no keys for decoding it. The malicious people cannot read the secret information without stego key even after stealing images. They construct the cloud computing system in local network, and investigate about safety, security and so on with two servers and a number of iPad from hardware side. On this system, they implemented server-side and client-side applications with different algorithms like AES, DES, RSA, Blowfish and Random with steganography.

For further improvement, they will use machine learning and computer vision techniques for automatic image morphing. Using results obtained in machine learning and computer vision, they can generate cover images using any images selected or uploaded by users.

Birendra Goswami and Dr.S.N.Singh proposed symmetric and asymmetric cryptographic algorithm algorithms for data security optimization. In this study, public key cryptography using matrices is structurally and functionally divided into two basic parts: First part deals with the pre-processing of data including the two main processes of data shuffling and traversing of the data. The second part of the algorithm deals with the key generation, key agreement and encryption decryption processes. Hybrid approach is used to encrypt actual large messages using symmetric schemes (DES, AES, etc.) and the key is transported using asymmetric schemes (RSA). The symmetric or asymmetric encryption algorithms uses hash functions as an integral part for the message integrity. Here, The Public Key Cryptography with Matrices is a three-stage secured algorithm and has a constant complexity i.e. fixed number of multiplications irrespective of the key size given over the ring of integers.

S.Swarajyam, E.Madhukar and P.Sowmya Lakshmi implementation of data security in cloud computing using Linear Programming. They develop problem transformation

techniques that enables customers to secretly transform the original LP into some arbitrary while protecting sensitive input/output information. They also investigate duality theorem and derive a set of necessary and sufficient condition for result verification. Such a cheating resilience design can be bundled in the overall mechanism with close-to-zero additional overhead. Both security analysis and experiment results demonstrates the immediate practicality of the proposed mechanism. They plan to investigate some interesting future work as follows: 1) devise robust algorithms to achieve numerical stability; 2) explore the sparsity structure of problem for further efficiency improvement; 3) establish formal security framework; 4) extend our result to non-linear programming computation outsourcing in cloud.

Mrinal Kanti Sarkar and Trijit Chatterjee provided the technique of maintaining the data integrity. While data being sent to server is saved behind the images. So, the unauthorized access cannot perceive the data as it is hidden. Thus, this approach is good as it makes use of steganography using images for protecting the integrity of data. The security of data during transmission is not handled at all. The SanjoliSingla and Jasmeet Singh presented approach is to encrypt the data to achieve confidentiality and privacy. They used Rijndael Encryption Algorithm along with EAP- CHAP.

Aparjita Sidhu and Rajiv Mahajan proposed hybrid encryption which contains two algorithms one for plain text and another for already encrypted text. In this scheme, the plain text is first converted to whitened text, containing text in hexadecimal format using MD5, which is again converted to encrypted form using AES algorithm. This scheme is simple and can be easily implemented. But from security point of view its feasibility is questionable as extensive use of encryption algorithms is done but no care has been taken to secure the keys used for encrypting the data.

Varsha Yadav and Preeti Aggarwal proposed the strategy of fingerprinting based Recursive information hiding in cloud environment. This scheme describe the use of client fingerprints to encrypt user's data and again to decrypt while retrieving it. They used a first unique approach as no two persons can have the same fingerprints. Second is that, if this scheme is applied then it is not always possible that the person using the cloud services will have fingerprint machine and if not then extra money is required to purchase respective machines and to make this model work.

Vaibhav Khadilkar, Anuj Gupta and Bhavani Thuraisingham proposed and given a comprehensive description of a technique using Hive and Hadoop with XACML policy to make the scheme work in a convenient way. However, to perform the action storage space and secure access to shared data are common issues.

VII CONCLUSION

Cloud computing services are used by larger and smaller scale organization. As everything is stores on cloud through internet, certainly the traditional security problems such as security vulnerabilities, virus and hack attack threat can meet to the cloud system. This paper describes the brief study of cloud computing deployment and service models, characteristics and different security and privacy related research papers. Top security concerns of cloud computing found in this study are data loss, data leakage, client's trust, user's authentication, malicious users handling, and hijacking of sessions while accessing data. We can conclude that security is the biggest stumbling block in wide acceptance of cloud computing. From user point of view cloud computing is suffering from server security threats. Here, we have focused on ant colony optimization, cryptography and steganography techniques. We will implement system for cloud security enhancement using ACO algorithm as it is the best way to find out the shortest path between two points through hurdle randomly selected by the user.

REFERENCES

1. Barrie Sosinsky, "Cloud Computing Bible", book Published by Wiley Publishing, Inc.
2. *Hassan, Qusay,* "Demystifying Cloud Computing", *The Journal of Defence Software Engineerin, 2011.*
3. *Peter Mell, Timothy Grance, ―The NIST Definition of Cloud Computing‖, Jan, 2011.*
4. Raj Kumar, "Research on Cloud Computing Security Threats using Data Transmission", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 1, January 2015.
5. MohsinNazir, "Cloud Computing: Overview & Current Research Challenges", IOSR Journal of Computer Engineering (IOSR-JCE) ISSN: 2278-0661, ISBN: 2278-8727Volume 8, Issue 1, PP 14-22, Nov- Dec. 2012.
6. MutumZicoMeetei, Anita Goel, "Security Issues in Cloud Computing".
7. Abdul Wahid Khan, SiffatUllah Khan, Muhammad Ilyas, Muhammad IlyasAzeem, "A Literature Survey on Data Privacy/ Protection Issues and Challenges in Cloud Computing ", IOSRJCE, Volume 1, Issue 3, PP 28-36, May-June 2012, ISSN : 2278-0661.
8. Ramasami S., Umamaheswari P., "Survey on Data Security Issues and Data Security Models in Cloud Computing", IJEIT, Volume 1, Issue 3, March 2012.
9. L. Ertaul, S. Singhal, and G. Saldamli, "Security Challenges in Cloud Computing".
10. Hitesh Hasija, Rahul Katarya, "Secure Code Assignment to Alphabets Using Modified Ant Colony Optimization along with Compression", IEEE, 978-1-4799-3080-7114, 2014.
11. K.Sriprasadh, M.Prakash Kumar, "Ant Colony Optimization Technique for Secure Various Data Retrieval in Cloud Computing", IJCSIT, Vol. 5 (6), 7528-7531, 2014.